



FortiManager - Administration Guide

Version 5.6.7

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



December 6, 2018

FortiManager 5.6.7 Administration Guide

02-567-400706-20181206

TABLE OF CONTENTS

Change Log	16
Introduction	17
FortiManager features	17
FortiManager feature set	17
FortiAnalyzer feature set	18
About this document	18
FortiManager documentation	18
What's New in FortiManager	20
FortiManager 5.6.7	20
FortiManager 5.6.6	20
FortiManager 5.6.5	20
FortiManager 5.6.4	20
FortiManager 5.6.3	20
FortiAP Manager per-device management option	21
FortiManager 5.6.2	21
Virtual wire pair policy support	21
SDN Connector for VMware NSX and Cisco ACI	21
FortiManager 5.6.1	21
Upgrade - One step ADOM upgrade to 5.6.1	21
FOS-VM HA Cluster Support	21
FortiSwitch Manager Improvements	21
Configurable FortiGuard server location from System Settings	22
FortiManager 5.6.0	22
Security Fabric management	22
Policy packages	23
VPN Manager	23
FortiAP Manager performance improvements	23
FortiGuard Package management usability	24
FMG-VM minimum configuration check	24
Add-on license for high-end appliances	24
FortiManager Architecture	25
Inside the FortiManager system	26
Communication protocols and devices	26
Object database and devices	27
ADOMs and devices	28
Operations	30
Key features of the FortiManager system	31
Security Fabric	31
Configuration revision control and tracking	31
Centralized management	31
Administrative domains	31

Local FortiGuard service provisioning	32
Firmware management	32
Scripting	32
Logging and reporting	32
Fortinet device life cycle management	32
GUI	33
Connecting to the GUI	33
GUI overview	34
Panes	35
Color themes	36
Full-screen mode	36
Switching between ADOMs	37
Using the right-click menu	37
Avatars	37
Showing and hiding passwords	38
Security considerations	38
Restricting GUI access by trusted host	38
Other security considerations	38
Restarting and shutting down	38
Getting Started	40
Configuring the FortiManager	40
Adding devices	40
Installing to managed devices	41
Enabling central management	41
Monitoring managed devices	42
Network	43
Configuring network interfaces	43
Disabling ports	44
Changing administrative access	45
Static routes	45
RAID Management	46
Supported RAID levels	46
Configuring the RAID level	49
Monitoring RAID status	49
Checking RAID from command line	50
Swapping hard disks	51
Adding hard disks	52
Administrative Domains	53
Default ADOMs	53
Organizing devices into ADOMs	53
Enabling and disabling the ADOM feature	54
ADOM device modes	55

ADOM modes	55
Managing ADOMs	56
Creating ADOMs	57
Assigning devices to an ADOM	59
Assigning VDOMs to an ADOM	59
Assigning administrators to an ADOM	60
Editing an ADOM	60
Deleting ADOMs	61
ADOM versions	61
Global database version	62
Concurrent ADOM access	63
Locking an ADOM	64
Upgrading an ADOM	64
Workflow Mode	65
Enable or disable workflow mode	65
Workflow approval	66
Workflow sessions	67
Administrators	73
Trusted hosts	73
Monitoring administrators	73
Disconnecting administrators	74
Managing administrator accounts	74
Creating administrators	75
Editing administrators	78
Deleting administrators	78
Restricted administrators	79
Administrator profiles	85
Permissions	86
Creating administrator profiles	89
Editing administrator profiles	91
Deleting administrator profiles	91
Authentication	91
Public Key Infrastructure	91
Managing remote authentication servers	93
LDAP servers	94
RADIUS servers	96
TACACS+ servers	96
Remote authentication server groups	97
Global administration settings	98
Password policy	100
Password lockout and retry attempts	101
GUI language	101
Idle timeout	102
Two-factor authentication	102
Configuring FortiAuthenticator	102

Configuring FortiManager	105
Device Manager	106
ADOMs	107
Adding devices	107
Adding devices using the wizard	108
Adding devices manually	115
Add a VDOM to a device	116
Adding a security fabric group	116
Import policy wizard	117
Adding FortiAnalyzer devices	119
Adding FortiAnalyzer devices with the wizard	120
Importing devices	123
Importing detected devices	123
Importing and exporting device lists	124
Configuring devices	124
Configuring a device	125
Out-of-Sync device	126
Configuring VDOMs	126
Using the device dashboard	129
View system dashboard for managed/logging devices	129
View system interfaces	131
CLI-Only Objects menu	131
System dashboard widgets	131
Installing to devices	134
Using the Install Wizard to install policy packages and device settings	134
Using the Install Wizard to install device settings only	136
View a policy package diff	136
Managing devices	137
Using the quick status bar	138
Customizing columns	138
Refreshing a device	138
Editing device information	139
Deleting a device	141
Replacing a managed device	141
Setting unregistered device options	142
Using the CLI console for managed devices	142
Displaying security fabric topology	143
Managing device configurations	143
View configurations for device groups	143
Checking device configuration status	145
Managing configuration revision history	147
Device groups	150
Default device groups	150
Add device groups	150
Manage device groups	150

Firmware	151
View firmware for device groups	151
Upgrade firmware for device groups	151
Firmware Management	152
License	153
View licenses for device groups	153
License Management	153
Add-on license	155
Provisioning Templates	155
System templates	155
Threat Weight templates	157
Certificate templates	158
Scripts	159
Enabling scripts	160
Configuring scripts	161
CLI script group	166
Script syntax	167
Script history	171
Script samples	171
SD-WAN Load Balance	192
Enabling central SD-WAN	192
Manage SD-WAN load balancing profiles	193
Creating SD-WAN load balancing profiles	193
Manage profiles for checking WAN link status	194
Creating profiles for checking WAN link status	194
FortiExtender	195
Centrally managed	195
FortiMeter	197
Overview	197
Points	198
Authorizing metered VMs	198
Monitoring VMs	199
FortiGate chassis devices	200
Viewing chassis dashboard	201
Log and file storage	205
Disk space allocation	205
Log and file workflow	205
Automatic deletion	207
Logs for deleted devices	207
Log storage policy	208
Configure log storage	209
Storage statistics	210
Policy & Objects	212
About policies	213
Policy theory	214

Global policy packages	215
Policy workflow	215
Provisioning new devices	215
Day-to-day management of devices	216
Display options	216
Managing policy packages	217
Create new policy packages	217
Create new policy package folders	218
Edit a policy package or folder	219
Clone a policy package	219
Remove a policy package or folder	220
Assign a global policy package	220
Install a policy package	221
Reinstall a policy package	221
Schedule a policy package install	223
Export a policy package	224
Policy package installation targets	224
Perform a policy consistency check	226
View logs related to a policy rule	227
Concurrent policy package access	227
Managing policies	228
Creating policies	230
Editing policies	231
IP policies	237
Virtual wire pair policy	242
NAT policies	244
Proxy policy	246
Central SNAT	248
Central DNAT	249
DoS policy	255
Interface policy	257
Multicast policy	258
Local in policy	259
Traffic shaping policy	260
Managing objects and dynamic objects	261
Create a new object	262
Map a dynamic object	263
Modify an existing Interface-Zone Mapping	264
Map a dynamic device group	264
Remove an object	265
Edit an object	265
Push to device	266
Clone an object	266
Search objects	267
Find unused objects	267
Find and merge duplicate objects	267

CLI-Only objects	267
FortiToken configuration example	268
FSSO user groups	268
Interface mapping	271
VIP mapping	271
Fortinet SDN Connector	271
Fortinet SDN Connector and VMware NSX	272
Fortinet SDN Connector and ACI	272
Configuring SDN Connector objects	273
Importing security groups to SDN Connector objects	274
Configuring virtual wire pairs	275
ADOM revisions	275
VPN Manager	279
Overview	279
Enabling central VPN management	280
DDNS support	281
IPsec VPN Communities	282
Managing IPsec VPN communities	282
Creating IPsec VPN communities	282
VPN community settings	284
Monitoring IPsec VPN tunnels	291
Map View	291
IPsec VPN gateways	293
Managing VPN gateways	293
Creating managed gateways	293
Creating external gateways	298
VPN security policies	300
Defining policy addresses	300
Defining security policies	300
SSL VPN	301
Manage SSL VPNs	301
Portal profiles	304
Monitor SSL VPNs	310
AP Manager	311
Managed APs	311
Quick status bar	312
Managing APs	313
FortiAP groups	317
Authorizing and deauthorizing FortiAP devices	318
Assigning profiles to FortiAP devices	318
Rogue APs	318
Connected clients	320
Monitoring AP devices	321
Clients Monitor	321

Health Monitor	322
Map View	323
WiFi templates	324
AP profiles	324
SSIDs	330
WIDS profiles	336
FortiClient Manager	340
How FortiManager fits into endpoint compliance	341
FortiTelemetry	341
Viewing devices	342
Enabling FortiTelemetry on interfaces	342
Enabling endpoint control on interfaces	343
Assigning FortiClient profile packages to devices	343
Monitor	343
Monitoring FortiClient endpoints	344
Monitoring FortiClient endpoints by compliance status	345
Monitoring FortiClient endpoints by interface	345
Exempting non-compliant FortiClient endpoints	345
FortiClient profiles	346
Viewing profile packages	346
Viewing FortiClient profiles	347
Creating FortiClient profile packages	347
Creating FortiClient profiles	348
Editing FortiClient profiles	351
Deleting FortiClient profiles	351
Importing FortiClient profiles	352
Assigning profile packages	352
FortiGuard	353
Settings	354
Connecting the built-in FDS to the FDN	357
Operating as an FDS in a closed network	358
Configuring devices to use the built-in FDS	360
Matching port settings	361
Handling connection attempts from unregistered devices	361
Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS	362
Configuring FortiGuard services	362
Enabling push updates	362
Enabling updates through a web proxy	364
Overriding default IP addresses and ports	364
Scheduling updates	365
Accessing public FortiGuard web and email filter servers	366
Logging events related to FortiGuard services	366
Logging FortiGuard antivirus and IPS updates	366
Logging FortiGuard web or email filter events	367

Restoring the URL or antispam database	368
Licensing status	368
Package management	369
Receive status	369
Service status	370
Query server management	371
Receive status	371
Query status	372
Firmware images	373
FortiSwitch Manager	375
Managed Switches	375
Quick status bar	376
Managing FortiSwitches	376
Authorizing and deauthorizing FortiSwitch devices	379
Assigning templates to FortiSwitch devices	380
Monitoring FortiSwitch devices	380
FortiSwitch Templates	381
FortiSwitch templates	381
FortiSwitch VLANs	384
FortiAnalyzer Features	390
Enable or disable FortiAnalyzer features	391
Viewing policy rules	391
FortiView	393
How ADOMs affect the FortiView pane	393
Logs used for FortiView	393
FortiView summary list and description	393
Using FortiView	397
FortiView Summary	397
Viewing FortiView summaries	399
Filtering FortiView summaries	402
Viewing related logs	402
Exporting filtered summaries	402
FortiView Indicators of Compromise	403
Monitoring resource usage of devices	404
Examples of using FortiView	404
Finding application and user information	404
Finding unsecured wireless access points	404
Analyzing and reporting on network traffic	405
Viewing vulnerabilities with high severity and frequency	405
NOC	406
NOC Dashboard	406
Using the NOC dashboard	407
Customizing the NOC dashboard	408

NOC dashboards and widgets	409
Security Monitor	409
WiFi Monitor	410
System Performance	410
Log View	412
Types of logs collected for each device	412
Log messages	414
Viewing the log message list of a specific log type	414
Viewing log message details	414
Customizing displayed columns	415
Filtering log messages	415
Viewing historical and real-time logs	418
Viewing raw and formatted logs	418
Custom views	418
Downloading log messages	419
Creating charts	420
Log groups	420
Log browse	421
Importing a log file	422
Downloading a log file	422
Deleting log files	423
Event Management	424
How ADOMs affect events	424
Predefined event handlers	424
Logs used for events	424
Event handlers	424
Managing event handlers	425
List of predefined event handlers	425
Enabling event handlers	432
Creating custom event handlers	433
Create New Handler pane	434
Filtering event handlers	436
Searching event handlers	436
Resetting to factory defaults	436
Events	437
Event summaries	437
Filtered event list	438
Event details	438
Acknowledging events	439
Event calendar	439
Reports	441
How ADOMs affect reports	441
Predefined reports, templates, charts, and macros	441
Logs used for reports	442
How charts and macros extract data from logs	442

How auto-cache works	442
Generating reports	442
Viewing completed reports	443
Enabling auto-cache	443
Grouping reports	444
Retrieving report diagnostic logs	444
Auto-Generated Reports	445
Scheduling reports	445
Creating reports	445
Creating reports from report templates	445
Creating reports by cloning and editing	446
Creating reports without using a template	447
Reports Settings tab	447
Customizing report cover pages	449
Reports Layout tab	450
Filtering report output	454
Managing reports	454
Organizing reports into folders	455
Importing and exporting reports	455
Report template library	456
Creating report templates	456
Viewing sample reports for predefined report templates	457
Managing report templates	457
List of report templates	458
Chart library	460
Creating charts	460
Managing charts	462
Macro library	463
Creating macros	463
Managing macros	464
Datasets	465
Creating datasets	465
Viewing the SQL query for an existing dataset	466
SQL query functions	467
Managing datasets	467
Output profiles	468
Creating output profiles	468
Managing output profiles	469
Report languages	469
Predefined report languages	470
Adding language placeholders	470
Managing report languages	470
Report calendar	471
Viewing all scheduled reports	471
Managing report schedules	471

System Settings	473
Dashboard	473
Customizing the dashboard	475
System Information widget	475
System Resources widget	481
License Information widget	482
Unit Operation widget	483
CLI Console widget	483
Alert Messages Console widget	484
Log Receive Monitor widget	484
Insert Rate vs Receive Rate widget	485
Log Insert Lag Time widget	485
Receive Rate vs Forwarding Rate widget	486
Disk I/O widget	486
Logging Topology	487
High Availability	488
Configuring HA options	490
Monitoring HA status	494
Upgrading the FortiManager firmware for an operating cluster	495
Certificates	495
Local certificates	496
CA certificates	498
Certificate revocation lists	500
Fetcher Management	501
Fetching profiles	501
Fetch requests	502
Synchronizing devices and ADOMs	504
Fetch monitoring	505
Event Log	505
Event log filtering	507
Task Monitor	508
SNMP	509
SNMP agent	510
SNMP v1/v2c communities	511
SNMP v3 users	514
SNMP MIBs	515
SNMP traps	516
Fortinet & FortiManager MIB fields	517
Mail Server	518
Syslog Server	520
Meta Fields	521
Device logs	522
Configuring rolling and uploading of logs using the GUI	523
Configuring rolling and uploading of logs using the CLI	525
File Management	526

Advanced Settings	527
-------------------------	-----

Change Log

Date	Change Description
2018-12-06	Initial release.

Introduction

FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, FortiWiFi, and FortiAP devices. Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), efficiently applying policies and distributing content security/firmware updates. FortiManager is one of several versatile Network Security Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

FortiManager features

FortiManager provides the following features:

- Provides easy centralized configuration, policy-based provisioning, update management, and end-to-end network monitoring for your Fortinet installation,
- Segregate management of large deployments easily and securely by grouping devices and agents into geographic or functional ADOMs,
- Manage units in a Fortinet Security Fabric group as if they were a single device and display the security fabric topology,
- Reduce your management burden and operational costs with fast device and agent provisioning, detailed revision tracking, and thorough auditing capabilities,
- Easily manage complex mesh and star VPN environments while leveraging FortiManager as a local distribution point for software and policy updates,
- Seamless integration with FortiAnalyzer appliances provides in-depth discovery, analysis, prioritization and reporting of network security events,
- Quickly create and modify policies/objects with a consolidated, drag and drop enabled, in-view editor,
- Script and automate device provisioning, policy pushing, etc. with JSON APIs or build custom web portals with the XML API,
- Leverage powerful device profiles for mass provisioning and configuration of managed devices,
- Centrally control firmware upgrades and content security updates from FortiGuard Center Threat Research & Response,
- Deploy with either a physical hardware appliance or virtual machine with multiple options to dynamically increase storage

FortiManager system architecture emphasizes reliability, scalability, ease of use, and easy integration with third-party systems.

FortiManager feature set

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- AP Manager

- FortiClient Manager
- VPN Manager
- FortiGuard
- FortiSwitch Manager
- System Settings

FortiAnalyzer feature set

The FortiAnalyzer feature set can be enabled in FortiManager. The FortiAnalyzer feature set includes the following panes:

- FortiView
- NOC
- Log View
- Event Management
- Reports



The FortiAnalyzer feature set is disabled by default. To enable the features, turn it on from the dashboard (see [System Information widget on page 475](#)), or use the following CLI commands:

```
config system global
    set faz-status enable
end
```

Changing faz status will affect FAZ feature in FMG. If you continue, system will reboot to add/remove FAZ feature.

```
Do you want to continue? (y/n) y
```

About this document

This document describes how to configure and manage your FortiManager system and the devices that it manages.

The FortiManager documentation assumes that you have one or more FortiGate units and documentation for the FortiGate unit. It also assumes that you are familiar with configuring your FortiGate units before using the FortiManager system. Where FortiManager system features or parts of features are identical to the FortiGate unit's, the FortiManager system documentation refers to the FortiGate unit documentation for further configuration assistance with that feature.

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager Compatibility*

This document identifies FortiManager software support for FortiOS.

- *FortiManager Release Notes*

This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

- *FortiManager Upgrade Guide*

This document describes how to upgrade FortiManager.

- *FortiManager device QuickStart Guides*

These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager Graphical User Interface (GUI).

- *FortiManager VM Install Guide*

This document describes installing FortiManager VM in your virtual environment.

- *FortiManager Administration Guide*

This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configure and manage the FortiGate VPN policies, monitor the status of the managed devices, view and analyze the FortiGate logs, update the virus and attack signatures, provide web filtering and email filter service to the licensed FortiGate units as a local FortiGuard Distribution Server (FDS), control firmware revisions and update the firmware images of the managed units.

- *FortiManager Online Help*

You can get online help from the FortiManager GUI. FortiManager online help contains detailed procedures for using the FortiManager GUI to configure and manage FortiGate units.

- *FortiManager CLI Reference*

This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.

- *FortiManager and FortiAnalyzer Event Log Reference*

This document describes the log messages available with FortiManager when local logging is enabled.

- *FortiManager JSON API Reference*

This document lists all of the objects available with the FortiManager JSON Application Programming Interface. The document is only available on the FNDN site at <https://fndn.fortinet.net/>.

- *FortiManager JSON API Diff*

This document lists all of the objects that were added, modified, and removed between the current and previous release of the FortiManager JSON Application Programming Interface. The document is only available on the FNDN site at <https://fndn.fortinet.net/>.

- *FortiManager XML API Reference*

This document describes how to use the legacy XML-based FortiManager Application Programming Interface to obtain information from the FortiManager unit.

What's New in FortiManager

FortiManager version 5.6 includes the following new features and enhancements. Always review all sections in the *FortiManager Release Notes* prior to upgrading your device.



Not all features/enhancements listed below are supported on all models.

FortiManager 5.6.7

FortiManager 5.6.7 includes no new features.

FortiManager 5.6.6

FortiManager 5.6.6 includes no new features.



Enabling the VPN manager does not delete previously configured VPN configuration on managed FortiGate devices in that ADOM.

FortiManager 5.6.5

FortiManager 5.6.5 includes no new features.

FortiManager 5.6.4

FortiManager 5.6.4 includes no new features.

FortiManager 5.6.3

FortiManager 5.6.3 includes the following new features and enhancements:

FortiAP Manager per-device management option

FortiAP Manager now supports a new per-device AP management option. When this option is enabled, the WiFi settings are managed at each FortiGate device level. The Central WiFi settings of the ADOM are not applied to the per-device managed APs.

FortiManager 5.6.2

FortiManager 5.6.2 includes the following new features and enhancements:

Virtual wire pair policy support

FortiManager now supports the addition of Virtual Wire Pair policies. You can create Virtual Wire Pair objects from *Object Configurations -> Interface* and then use the objects in the Virtual Wire Pair policies. See [Virtual wire pair policy on page 242](#)

SDN Connector for VMware NSX and Cisco ACI

You can now create VMware NSX and Cisco ACI connectors from FortiManager, use the connectors to dynamically learn NSX or ACI objects, import the objects to its local object database, and then use the objects in its central policies. See [Fortinet SDN Connector and VMware NSX on page 272](#) and [Fortinet SDN Connector and ACI on page 272](#).

FortiManager 5.6.1

FortiManager 5.6.1 includes the following new features and enhancements:

Upgrade - One step ADOM upgrade to 5.6.1

One step procedure to upgrade a 5.4-based ADOM to a 5.6-based ADOM. See [Upgrading an ADOM on page 64](#).

FOS-VM HA Cluster Support

FOS-VM HA clusters are now supported by FortiManager. Install and retrieve FOS-VM configurations, authorize UTM services to FOS-VM members, provide metering service for FOS-VM HA cluster, and upgrade FOS-VM firmware.

FortiSwitch Manager Improvements

FortiSwitch Manager now supports:

- Trunk interface creation
- DHCP Snooping
- IGMP Network Traffic Snooping
- STP State
- Loop-guard/loop-guard timeout
- Port speed/status

See [FortiSwitch Manager on page 375](#) for more information.

Configurable FortiGuard server location from System Settings

You can now view the list of connected FortiGuard update servers from the *License Information* widget and update the list by selecting a preferred server location. See [License Information widget on page 482](#).

FortiManager 5.6.0

FortiManager 5.6.0 includes the following new features and enhancements:

Security Fabric management

Managed FortiGate Security Fabric cluster

You can now manage FortiGates in a Security Fabric cluster as if they are a single device. See [Adding a security fabric group on page 116](#).

You can also view the topology of the FortiGate Security Fabric cluster from *Device Manager*. See [Displaying security fabric topology on page 143](#).

FortiSwitch Manager

A new FortiSwitch Manager module that supports provisioning templates, central deployments and status monitoring for managed switches is available. See [FortiSwitch Manager on page 375](#).

Managed FortiAnalyzer

You can now use the new Add FortiAnalyzer device wizard to add a FortiAnalyzer unit to FortiManager to better support managed devices with logging enabled. See [Adding FortiAnalyzer devices on page 119](#).



You cannot add a FortiAnalyzer unit to FortiManager when ADOMs are enabled and ADOM mode is set to *Advanced*.

When you add a FortiAnalyzer device to FortiManager with ADOMs disabled, all devices with logging enabled will automatically send logs to the FortiAnalyzer device. You can add only one FortiAnalyzer device to FortiManager, and the FortiAnalyzer device limit must be equal to or greater than the number of devices managed by FortiManager.

When you add a FortiAnalyzer device to FortiManager with ADOMs enabled, all devices with logging enabled in the ADOM will automatically send logs to the FortiAnalyzer device. You can add only one FortiAnalyzer device to each ADOM, and the FortiAnalyzer device limit must be equal to or greater than the number of devices managed by FortiManager ADOM.

After you add a FortiAnalyzer device to FortiManager by using the Add FortiAnalyzer device wizard, you can use FortiManager to remotely access *FortiView*, *Log View*, *Events Managements*, and *Reports* on the managed FortiAnalyzer unit.

Policy packages

Central DNAT

Central DNAT is now available on a per policy package level. You can add a central DNAT entry by creating a new Virtual IP or by using an existing Virtual IP. These DNAT entries are shared amongst all the policy packages. See [Central DNAT on page 249](#).

Traffic shaping policy package for ADOMs

FortiManager now supports global traffic shaping policies that allow both header and footer traffic shaping policies.

FortiManager also supports traffic shaping policy packages at the ADOM level.

See [Traffic shaping policy on page 260](#).

VPN Manager

Set priority on VPN Gateway interface

You can set priority on VPN Gateway Interface from the FortiManager GUI by using the *Advanced Options* section. The priority information is now saved in the generated VPN routes. See [VPN Manager on page 279](#).

VPN Gateways on Google map

Display VPN gateways on Google map and monitor the VPN tunnel traffic in real-time. See [Map View on page 291](#).

FortiAP Manager performance improvements

The performance of *AP Manager* for managing deployments with more than 10,000 FortiAP units has been improved. See [AP Manager on page 311](#).

FortiGuard Package management usability

You can view the service status by managed device or by installed package. See [Service status on page 370](#).

FMG-VM minimum configuration check

For FMG-VM running in VMware hypervisor, the FortiManager GUI displays a warning if the VM installation does not meet the minimum required 2x vCPU and 4GB memory. See [System Resources widget on page 481](#).

Add-on license for high-end appliances

- Allows additional devices/vdom on high-end appliances; additional devices are added in batches of 100
- Up to 100,000 devices/vdoms maximum on FMG-3900E
- Up to 8,000 devices/vdoms maximum on FMG-3000F

FortiManager Architecture

FortiManager is an integrated platform for the centralized management of products in a Fortinet security infrastructure. FortiManager provides centralized policy-based provisioning, configuration and update management for FortiGate, FortiWiFi, FortiAP, and other devices. For a complete list of supported devices, see the *FortiManager Release Notes*.

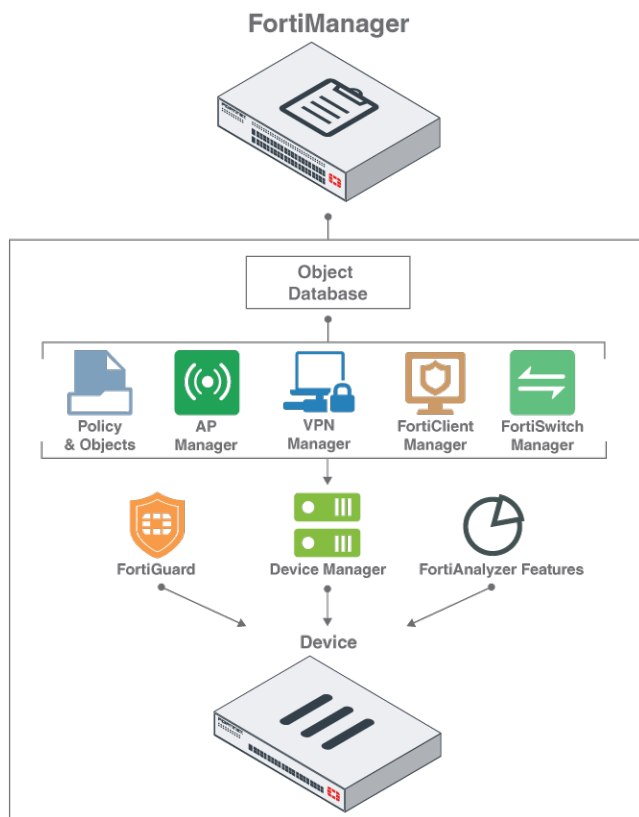
To reduce network delays and to minimize external Internet usage, a FortiManager installation can also act as an on-site FortiGuard Distribution Server (FDS) for your managed devices and FortiClient agents to download updates to their virus and attack signatures, and to use the built-in web filtering and email filter services.

You can also optionally enable the FortiAnalyzer features, which enables you to analyze logs for managed devices and generate reports.

FortiManager scales to manage up to 5000 devices and virtual domains (VDOMs) from a single FortiManager interface. It is primarily designed for medium to large enterprises and managed security service providers.

Using a FortiManager device as part of an organization's Fortinet security infrastructure can help minimize both initial deployment costs and ongoing operating expenses. It allows fast device provisioning, detailed revision tracking, and thorough auditing.

Following is a diagram that shows an overview of the main FortiManager elements: Device Manager, FortiGuard, and FortiAnalyzer features. FortiManager includes a central database that stores elements for Policy & Objects, AP Manager, VPN Manager, FortiClient Manager, and FortiSwitch Manager, and you can install these elements to devices through Device Manager.

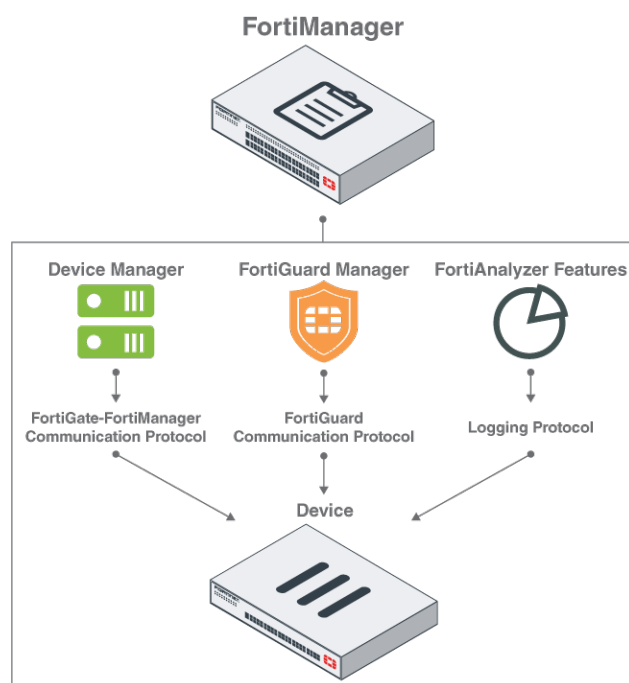


Inside the FortiManager system

FortiManager is a robust system with multiple communication protocols and layers to help you effectively manage your Fortinet security infrastructure.

Communication protocols and devices

FortiManager communicates with managed devices by using several protocols. *Device Manager*, *FortiGuard Manager*, and *FortiAnalyzer Features* each use a different protocol to communicate with managed devices.



Device Manager

Device Manager contains all devices that are managed by the FortiManager unit. You can create new device groups, provision and add devices, and install policy packages and device settings. *Device Manager* communicates with devices by using the FortiGate-FortiManager (FGFM) protocol. See [Device Manager on page 106](#).

FortiGuard Manager

FortiGuard Manager communicates with devices by using the FortiGuard protocol.

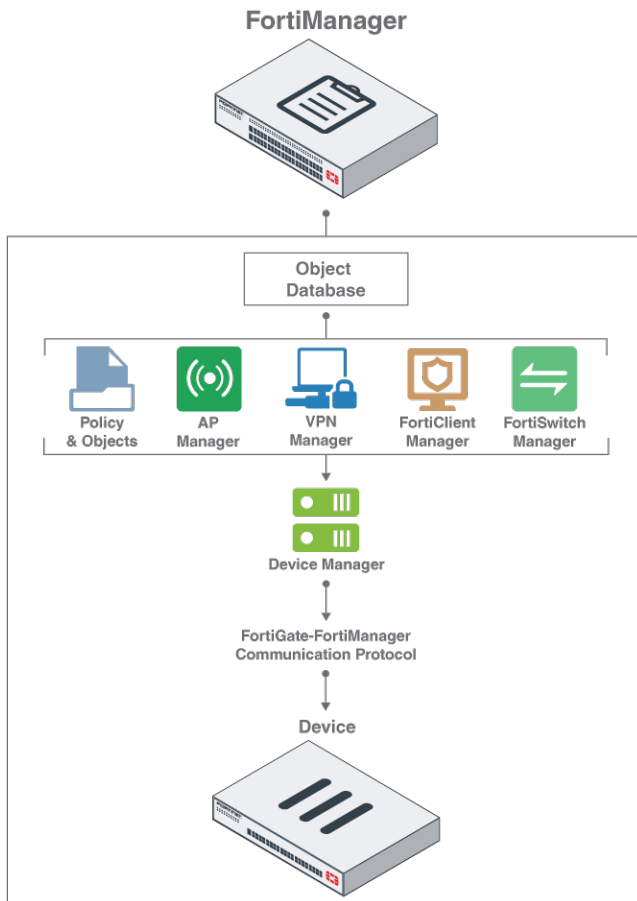
FortiAnalyzer features

When FortiAnalyzer features are enabled for the FortiManager unit, the *FortiView*, *NOC*, *Log View*, *Event Management*, and *Reports* panes are available. FortiAnalyzer features include tools for viewing and analyzing log messages, and the feature communicates with devices by using the logging protocol.

Object database and devices

FortiManager includes an object database to store all of the objects that you create. You can use the objects in the following panes and apply the objects to devices:

- *Policy & Objects*
- *AP Manager*
- *VPN Manager*
- *FortiClient Manager*
- *FortiSwitch Manager*



Policy & Objects

The *Policy & Objects* pane contains all of your global and local policy packages and objects, and configuration revisions. Objects created for the *Policy & Objects* pane are stored in the objects database. See [Policy & Objects on page 212](#).

AP Manager

The *AP Manager* pane lets you view and configure FortiAP access points as well as FortiExtender wireless WAN extenders. Objects created for the *AP Manager* pane are stored in the objects database. See [AP Manager on page 311](#).

VPN Manager

The *VPN Manager* pane lets you centrally manage IPsec VPN and SSL-VPN settings. Objects created for the *VPN Manager* pane are stored in the objects database. See [VPN Manager on page 279](#).

FortiClient Manager

The *FortiClient Manager* pane lets you manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices. Objects created for the *FortiClient Manager* pane are stored in the objects database. See [FortiClient Manager on page 340](#).

FortiSwitch Manager

The *FortiSwitch Manager* pane lets you manage and monitor FortiSwitch devices, and configure FortiSwitch templates and VLANs. Objects created for the *FortiSwitch Manager* pane are stored in the objects database. See [FortiSwitch Manager on page 375](#).

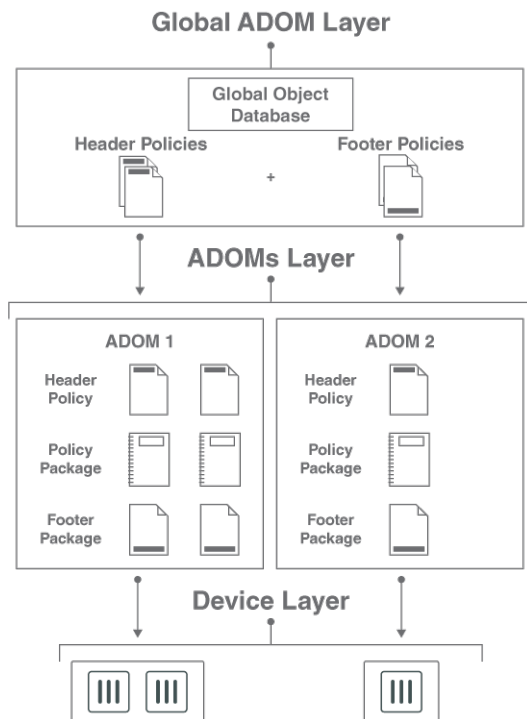
ADOMs and devices

The *Device Manager* pane is used to install policy packages to devices. When ADOMs are enabled, the *Device Manager* pane is used to install policy packages to the devices in an ADOM.

Policy packages can include header policies and footer policies. You can create header and footer policies by using the global ADOM. The global ADOM allows you to create header and footer policies once, and then assign the header and footer policies to multiple policy packages in one or more ADOMs.

For example, a header policy might block all network traffic to a specific country, and a footer policy might start antivirus software. Although you have unique policy packages in each ADOM, you might want to assign the same header and footer policies to all policy packages in all ADOMs.

Following is a visual summary of the process and a description of what occurs in the global ADOM layer, ADOM layer, and device manager layer.



Global ADOM layer

The global ADOM layer contains two key pieces: the global object database and all header and footer policies.

Header and footer policies are used to envelop policies within each individual ADOM. These are typically invisible to users and devices in the ADOM layer. An example of where this would be used is in a carrier environment, where the carrier would allow customer traffic to pass through their network but would not allow the customer to have access to the carrier's network assets.

ADOM layer

The ADOM layer is where FortiManager manages individual devices, VDOMs, or groups of devices. It is inside this layer where policy packages and folders are created, managed, and installed on managed devices. Multiple policy packages and folders can be created here. The ADOM layer contains one common object database per ADOM, which contains information such as addresses, services, antivirus and attack definitions, and web filtering and email filter.

Device manager layer

The device manager layer records information on devices that are centrally managed by the FortiManager unit, such as the name and type of device, the specific device model, its IP address, the current firmware installed on the unit, the device's revision history, and its real-time status.

Operations

Install

The install operation pushes device configuration from the FortiManager to a FortiGate device.

The FortiManager compares the configuration information that it has with the current configuration on the FortiGate. It then pushes the necessary configuration changes to the FortiGate to ensure that the FortiGate is synchronized with the FortiManager.

The install operation can include only device settings, or device settings and policy packages.

For more information, see [Installing to devices on page 134](#).

Re-install

The re-install operation reinstalls a policy package on a FortiGate device. For more information, see [Reinstall a policy package on page 221](#).

Import

The import operation copies policies and policy-related objects from the device database into the ADOM, creating a policy package that reflects the current configuration of the FortiGate device.

For more information, see [Import policy wizard on page 117](#).

Retrieve

The retrieve operation retrieves the FortiGate configuration and stores it in the device database on the FortiManager.

Auto-Update

When there is a change on the FortiGate that is not initiated by an install operation, the FortiGate automatically sends the configuration changes to the FortiManager.

The auto-update operation is enabled by default. To disable auto-update and allow the administrator to accept or refuse updates, use the following CLI commands:

```
config system admin settings
  set auto-update disable
end
```

Auto-Backup

The auto-backup operation is similar to auto-update, but only available when the FortiManager is in backup mode. The FortiGate device will wait until the FortiGate admin user has logged out before performing the backup.

For more information, see [ADOM modes on page 55](#).

Auto-Retrieve

The auto-retrieve operation is only invoked if the FortiGate fails to initiate an auto-update operation. When the FortiManager detects a change on the FortiGate, it automatically retrieves the full configuration.

Refresh

The FortiManager queries the FortiGate to update that FortiGate's current synchronization status. For more information, see [Refreshing a device on page 138](#).

Revert

The revert operation loads a saved configuration revision into the device database. For more information, see [Managing configuration revision history on page 147](#).

Key features of the FortiManager system

Security Fabric

FortiManager can recognize a Security Fabric group of devices and display all units in the group on the *Device Manager* pane, and you can manage the units in the Security Fabric group as if they were a single device. See [Adding a security fabric group on page 116](#). You can also display the security fabric topology. See [Displaying security fabric topology on page 143](#).

Configuration revision control and tracking

Your FortiManager unit records and maintains the history of all configuration changes made over time. Revisions can be scheduled for deployment or rolled back to a previous configuration when needed.

Centralized management

FortiManager can centrally manage the configurations of multiple devices from a single console. Configurations can then be built in a central repository and deployed to multiple devices when required.

Administrative domains

FortiManager can segregate management of large deployments by grouping devices into geographic or functional ADOMs. See [Administrative Domains on page 53](#).

Local FortiGuard service provisioning

A FortiGate device can use the FortiManager unit for antivirus, intrusion prevention, web filtering, and email filtering to optimize performance of rating lookups, and definition and signature downloads. See [FortiGuard on page 353](#).

Firmware management

FortiManager can centrally manage firmware images and schedule managed devices for upgrade.

Scripting

FortiManager supports CLI or Tcl based scripts to simplify configuration deployments. See [Scripts on page 159](#).

Logging and reporting

FortiManager can also be used to log traffic from managed devices and generate Structured Query Language (SQL) based reports. FortiManager also integrates FortiAnalyzer logging and reporting features.

Fortinet device life cycle management

The management tasks for devices in a Fortinet security infrastructure follow a typical life cycle:

- *Deployment*: An administrator completes configuration of the Fortinet devices in their network after initial installation.
- *Monitoring*: The administrator monitors the status and health of devices in the security infrastructure, including resource monitoring and network usage. External threats to your network infrastructure can be monitored and alerts generated to advise.
- *Maintenance*: The administrator performs configuration updates as needed to keep devices up-to-date.
- *Upgrading*: Virus definitions, attack and data leak prevention signatures, web and email filtering services, and device firmware images are all kept current to provide continuous protection for devices in the security infrastructure.

See also [Getting Started on page 40](#).

GUI

You can use the GUI to configure most FortiManager settings, such as the date, time, and the host name. You can also use the GUI to reboot and shut down the FortiManager unit.

Connecting to the GUI

The FortiManager unit can be configured and managed using the GUI or the CLI. This section will step you through connecting to the unit via the GUI.

To connect to the GUI:

1. Connect the FortiManager unit to a management computer using an Ethernet cable.
2. Configure the management computer to be on the same subnet as the internal interface of the FortiManager unit:
 - IP address: 192.168.1.X
 - Netmask: 255.255.255.0
3. On the management computer, start a supported web browser and browse to `https://192.168.1.99`.
4. Type `admin` in the *Name* field, leave the *Password* field blank, and click *Login*.
5. If ADOMs are enabled, the *Select an ADOM* pane is displayed. Click an ADOM to select it.
The FortiManager home page is displayed.
6. Click a tile to go to that pane. For example, click the *Device Manager* tile to go to the *Device Manager* pane.



If the network interfaces have been configured differently during installation, the URL and/or permitted administrative access protocols (such as HTTPS) may no longer be in their default state.

For information on enabling administrative access protocols and configuring IP addresses, see [Configuring network interfaces on page 43](#).



If the URL is correct and you still cannot access the GUI, you may also need to configure static routes. For details, see [Static routes on page 45](#).

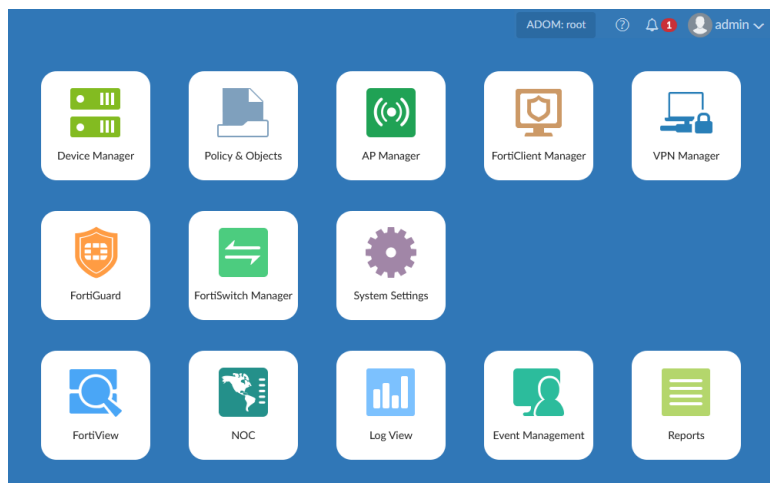


When the system is busy during a database upgrade or rebuild, you will receive a message in the GUI log-in pane. The message will include the estimated completion time.

After logging in for the first time, you should create an administrator account for yourself and assign the *Super_User* profile to it. Then you should log into the FortiManager unit by using the new administrator account. See [Managing administrator accounts on page 74](#) for information.

GUI overview

When you log into the FortiManager GUI, the following home page of tiles is displayed:



Select one of the following tiles to display the respective pane. The available tiles will vary, depending on the privileges of the current user.

Device Manager	Manage devices, VDOMs, groups, firmware images, device licenses, and scripts. You can also configure system, threat weight, and Certificate templates, and view real-time monitor data. See Device Manager on page 106 .
Policy & Objects	Configure policy packages and objects. For more information, see Policy & Objects on page 212 .
AP Manager	Configure and manage FortiAP access points. For more information, see AP Manager on page 311 .
FortiClient Manager	Manage FortiClient profiles and monitor FortiClient endpoints that are registered to FortiGate devices. See FortiClient Manager on page 340 .
VPN Manager	Configure and manage VPN connections. You can create VPN topologies and managed/external gateways. For more information, see VPN Manager on page 279 .
FortiGuard	Manage communication between devices and the FortiManager using the FortiGuard protocol. See FortiGuard on page 353 .
FortiSwitch Manager	Configure and manage FortiSwitch devices. For more information, see FortiSwitch Manager on page 375 .
FortiView	View summaries of log data in graphical formats. For example, you can view top threats to your network, top sources of network traffic, top destinations of network traffic and so on. For each summary view, you can drill down into details for the event. See FortiView on page 393 . This pane is only available when FortiAnalyzer features are enabled.

NOC	View network security, WiFi security, and system performance in real-time. You can select what activities to monitor in customizable dashboards. See NOC on page 406 . This pane is only available when FortiAnalyzer features are enabled.
Log View	View logs for managed devices. You can display, download, import, and delete logs on this page. You can also define custom views and create log groups. See Log View on page 412 . This pane is only available when FortiAnalyzer features are enabled.
Event Management	Configure and view events for logging devices. See Event Management on page 424 . This pane is only available when FortiAnalyzer features are enabled.
Reports	Generate reports. You can also configure report templates, schedules, and output profiles, and manage charts and datasets. See Reports on page 441 . This pane is only available when FortiAnalyzer features are enabled.
System Settings	Configure system settings such as network interfaces, administrators, system time, server settings, and others. You can also perform maintenance and firmware operations. See System Settings on page 473 .

The top-right corner of the home page includes a variety of possible selections:

HA status	If HA is enabled, the status is shown.
ADOM	If ADOMs are enabled, the required ADOM can be selected from the dropdown list. If enabled, ADOMs can also be locked or unlocked. The ADOMs available from the ADOM menu will vary depending on the privileges of the current user.
Help	Click to open the FortiManager online help, or view the <i>About</i> information for your device (Product, Version, and Build Number).
Notification	Click to display a list of notifications. Select a notification from the list to take action on the issue.
admin	Click to change the password or log out of the GUI.

Panes

In general, panes have four primary parts: the banner, toolbar, tree menu, and content pane.

Banner	Along the top of the page; includes the home button (Fortinet logo), tile menu, ADOM menu (when enabled), admin menu, notifications, and help button.
Tree menu	On the left side of the screen; includes the menus for the selected pane.

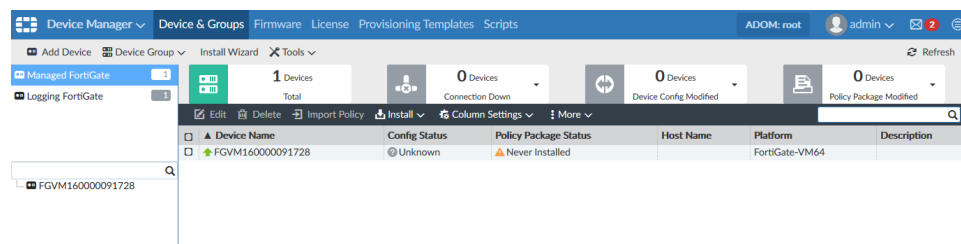
Content pane

Contains widgets, lists, configuration options, or other information, depending on the pane, menu, or options that are selected. Most management tasks are handled in the content pane.

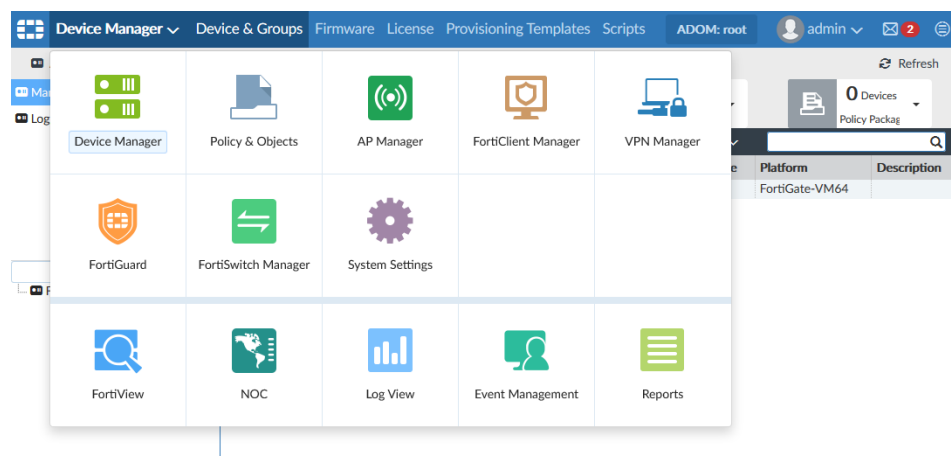
Toolbar

Directly above the content pane; includes options for managing content in the content pane, such as *Create New* and *Delete*.

The *Device Manager* pane includes a quick status bar on the top of the content pane that provides quick information on the state of the devices in the current device group. Clicking a status updates the content pane to display the relevant devices. See [Device Manager on page 106](#) for more information.



To switch between panes, either select the home button to return to the home page, or select the tile menu then select a new tile.



Color themes

You can choose a color theme for the FortiManager GUI. For example, you can choose a color, such as blue or plum, or you can choose an image, such as summer or autumn. See [Global administration settings on page 98](#).

Full-screen mode

You can view several panes in full-screen mode. When a pane is in full-screen mode, tree menu on the left side of the screen is hidden.

Click the *Full Screen* button in the toolbar to enter full-screen mode, and press the *Esc* key on your keyboard to exit full-screen mode.

Switching between ADOMs

When ADOMs are enabled, you can move between ADOMs by selecting an ADOM from the *ADOM* menu in the banner.

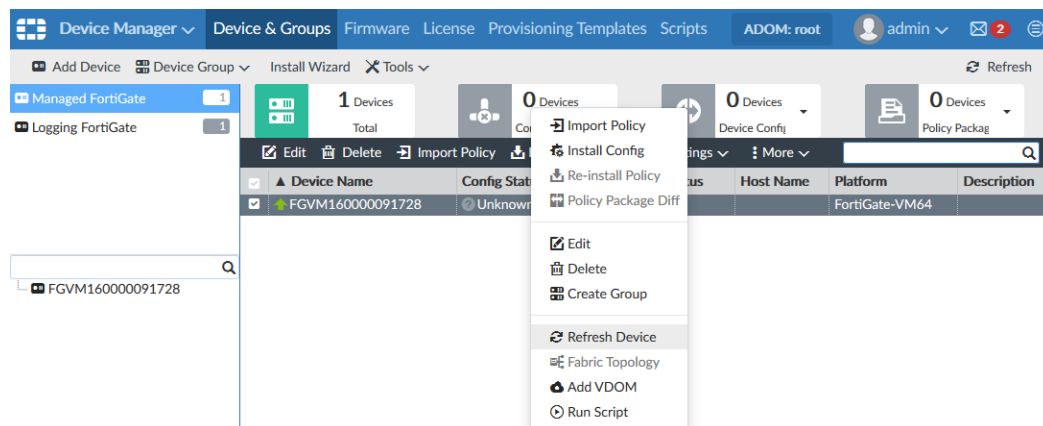


ADOM access is controlled by administrator accounts and the profile assigned to the administrator account. Depending on your account privileges, you might not have access to all ADOMs. See [Managing administrator accounts on page 74](#) for more information.

Using the right-click menu

Options are sometimes available using the right-click menu. Right-click an item in the content pane, or within some of the tree menus, to display the menu that includes various options similar to those available in the toolbar.

In the following example on the *Device Manager* pane, you can right-click a device in the content pane, and select *Install Config*, *Import Policy*, *Edit*, *Run Script*, and so on.



Avatars

When FortiClient sends logs to FortiManager with FortiAnalyzer features enabled, an avatar for each user can be displayed in the *Source* column in the *FortiView* and *Log View* panes. FortiManager can display an avatar when the following requirements are met:

- FortiClient is managed by FortiGate or FortiClient EMS with logging to FortiManager enabled.
- FortiClient sends logs and a picture of each user to FortiManager.

If FortiManager cannot find the defined picture, a generic, gray avatar is displayed.



You can also optionally define an avatar for FortiManager administrators. See [Creating administrators on page 75](#).

Showing and hiding passwords

In some cases you can show and hide passwords by using the toggle icon. When you can view the password, the *Toggle show password* icon is displayed:

Password 

When you can hide the password, the *Toggle hide password* icon is displayed:

Password 

Security considerations

You can take steps to prevent unauthorized access and restrict access to the GUI.

Restricting GUI access by trusted host

To prevent unauthorized access to the GUI you can configure administrator accounts with trusted hosts. With trusted hosts configured, the administrator user can only log into the GUI when working on a computer with the trusted host as defined in the administrator account. You can configure up to ten trusted hosts per administrator account. See [Administrators on page 73](#) for more details.

Other security considerations

Other security consideration for restricting access to the FortiManager GUI include the following:

- Configure administrator accounts using a complex passphrase for local accounts
- Configure administrator accounts using RADIUS, LDAP, TACACS+, or PKI
- Configure the administrator profile to only allow read/write permission as required and restrict access using read-only or no permission to settings which are not applicable to that administrator
- Configure the administrator account to only allow access to specific ADOMs as required
- Configure the administrator account to only allow access to specific policy packages as required.

Restarting and shutting down

Always use the operation options in the GUI or the CLI commands to reboot and shut down the FortiManager system to avoid potential configuration problems.

To restart the FortiManager unit from the GUI:

1. Go to *System Settings > Dashboard*.
2. In the *Unit Operation* widget, click the *Restart* button.
3. Enter a message for the event log, then click *OK* to restart the system.

To restart the FortiManager unit from the CLI:

1. From the CLI, or in the *CLI Console* widget, enter the following command:

```
execute reboot
```

The system will be rebooted.
Do you want to continue? (y/n)
2. Enter *y* to continue. The FortiManager system will restart.

To shutdown the FortiManager unit from the GUI:

1. Go to *System Settings > Dashboard*.
2. In the *Unit Operation* widget, click the *Shutdown* button.
3. Enter a message for the event log, then click *OK* to shutdown the system.

To shutdown the FortiManager unit from the CLI:

1. From the CLI, or in the *CLI Console* widget, enter the following command:

```
execute shutdown
```

The system will be halted.
Do you want to continue? (y/n)
2. Enter *y* to continue. The FortiManager system will shutdown.

To reset the FortiManager unit:

1. From the CLI, or in the *CLI Console* widget, enter the following command:

```
execute reset all-settings
```

This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
2. Enter *y* to continue. The device will reset to factory default settings and restart.

To reset logs and re-transfer all SQL logs to the database:

1. From the CLI, or in the *CLI Console* widget, enter the following command:

```
execute reset-sqllog-transfer
```

WARNING: This operation will re-transfer all logs into database.
Do you want to continue? (y/n)
2. Enter *y* to continue. All SQL logs will be resent to the database.

Getting Started

This chapter provides an overview of how to configure a FortiManager device. It also provides an overview of adding devices to FortiManager as well as configuring and monitoring managed devices.



After you configure IP addresses and administrator accounts for the FortiManager unit, you should log in again by using the new IP address and your new administrator account.

Configuring the FortiManager

Following is an overview of how to configure a FortiManager device.

To configure FortiManager devices:

1. Connect to the GUI. See [Connecting to the GUI on page 33](#).
2. Configure IP addresses. See [Configuring network interfaces on page 43](#).
3. Configure the RAID level, if the FortiManager unit supports RAID. See [RAID Management on page 46](#).

Adding devices

After you configure the FortiManager device, you should plan the network topology, configure ADOMs, configure administrative accounts, and then add the devices that you want to manage.

The number of devices that can be managed depends on the device model and license. An add-on license can be purchased for some high end devices to increase that number of device that can be managed. See [Add-on license on page 155](#) for more information.

It is recommended that you import the policy from the device when you add the device to FortiManager. FortiManager uses the imported policy to automatically create a policy package for that device.

To add devices:

1. Plan your network topology.
2. Configure administrative domains. See [Administrative Domains on page 53](#).
3. Configure administrator accounts. See [Managing administrator accounts on page 74](#).
4. Add devices to FortiManager. See [Adding devices on page 107](#).
5. If not done when you added the device, import the policy from each online device to FortiManager. See [Import policy wizard on page 117](#).

A policy package is automatically created for the device based on the policy. You can view the policy package on the *Policy & Objects* pane.



After initially importing policies from the device, all changes related to policies and objects should be made in *Policy & Objects* on the FortiManager.

Making changes directly on the FortiGate device will require reimporting policies to resynchronize the policies and objects.

Installing to managed devices

After you add devices to FortiManager, you can configure objects and policies, and use policy packages to install the objects and policies to one or more devices.

If you imported a policy from a device, you can edit and create policies for the imported policy package, and then install the updated policy package back to the device. Alternately you can create and configure a new policy package. You can install a policy package to multiple devices.

If you want to install device-specific settings, you can configure the settings by using the device dashboard on the *Device Manager* pane. When you install to the device, the device-specific settings are pushed to the device.

To install to devices:

1. Create or edit objects. See [Create a new object on page 262](#) or [Edit an object on page 265](#).
2. Create or edit policies in a policy package to select the objects. See [Creating policies on page 230](#) or [Editing policies on page 231](#).
You can create or edit policies in the policy package that was automatically created for the device when you imported its policy. Alternately, you can create a new policy package in which to define policies. See [Create new policy packages on page 217](#).
3. Ensure that the installation targets for the policy package include the correct devices. See [Policy package installation targets on page 224](#).
4. Edit device-specific settings by using the device dashboard on the *Device Manager* pane. See [Using the device dashboard on page 129](#).
5. Install the policy package and device settings to devices by using the Installation Wizard. See [Installing to devices on page 134](#).

Enabling central management

FortiManager includes the option to enable central management for each of the following elements:

- SD-WAN link load balance: see [SD-WAN Load Balance on page 192](#)
- VPN: see [VPN Manager on page 279](#)
- Access Points: see [AP Manager on page 311](#)

When central management is enabled, you can configure settings once, and then install the settings to one or more devices.

When central management is disabled, you must configure the settings for each device, and then install the settings to each device.

To use central management:

1. Enable central management for SD-WAN link load balance, FortiAP, and/or VPN.
2. Configure the settings.
3. Install the settings to one or more devices.

Monitoring managed devices

FortiManager includes many options for monitoring managed devices. Following is a sample of panes that you can use to monitor managed devices:

- Quick status bar—see [Using the quick status bar on page 138](#)
- Device dashboard—see [Using the device dashboard on page 129](#)
- Device configurations—see [Managing device configurations on page 143](#)
- Policy packages—see [Managing policy packages on page 217](#)
- *FortiClient Manager* pane—see [Monitoring FortiClient endpoints on page 344](#)
- *FortiSwitch Manager* pane—see [Monitoring FortiSwitch devices on page 380](#)

When optional centralized features are enabled, you can also use the following panes to monitor the centralized features for managed devices:

- *SD-WAN* pane—see [SD-WAN Load Balance on page 192](#)
- *AP Manager* pane—see [Monitoring AP devices on page 321](#)
- *VPN Manager* pane—see [VPN Manager on page 279](#)

When FortiAnalyzer features are enabled on the FortiManager device, you can also view and analyze log messages from managed devices by using the *FortiView*, *Log View*, *Event Management*, and *Reports* panes. See [FortiAnalyzer Features on page 390](#).

Network

The network settings are used to configure ports for the FortiManager unit. You should also specify what port and methods that an administrators can use to access the FortiManager unit. If required, static routes can be configured.

The default port for FortiManager units is port 1. It can be used to configure one IP address for the FortiManager unit, or multiple ports can be configured with multiple IP addresses for improved security.

You can configure administrative access in IPv4 or IPv6 and include settings for HTTPS, HTTP, PING, SSH, TELNET, SNMP, and Web Service.

You can prevent unauthorized access to the GUI by creating administrator accounts with trusted hosts. With trusted hosts configured, the administrator can only log in to the GUI when working on a computer with the trusted host as defined in the administrator account. For more information, see [Trusted hosts on page 73](#) and [Managing administrator accounts on page 74](#).

Configuring network interfaces

Fortinet devices can be connected to any of the FortiManager unit's interfaces. The DNS servers must be on the networks to which the FortiManager unit connects, and should have two different IP addresses.

If the FortiManager unit is operating as part of an HA cluster, it is recommended to configure interfaces dedicated for the HA connection / synchronization. However, it is possible to use the same interfaces for both HA and device management. The HA interface will have */HA* appended to its name.

The following port configuration is recommended:

- Use port1 for device log traffic, and disable unneeded services on it, such as SSH, TELNET, Web Service, and so on.
- Use a second port for administrator access, and enable HTTPs, Web Service, and SSH for this port. Leave other services disabled.

To configured port 1:

1. Go to *System Settings > Network*. The *System Network Management Interface* pane is displayed.

The screenshot shows the 'System Network Management Interface' configuration page for 'port1'. The interface includes the following fields and options:

- Name:** port1
- IP Address/Netmask:** 1.1.1.1/255.255.255.0
- IPv6 Address:** ::0
- Administrative Access:** ☒ HTTPS ☒ HTTP ☒ PING ☒ SSH ☒ TELNET ☐ SNMP ☐ Web Service
- IPv6 Administrative Access:** ☐ HTTPS ☐ HTTP ☐ PING ☐ SSH ☐ TELNET ☐ SNMP ☐ Web Service
- Service Access:** ☐ FortiGate Updates ☐ Web Filtering
- Default Gateway:** 1.1.1.1
- Primary DNS Server:** 1.1.1.1
- Secondary DNS Server:** 11.11.11.11

At the bottom, there are three tabs: 'All Interfaces', 'Routing Table', and 'IPv6 Routing Table'. An 'Apply' button is located at the bottom right of the configuration area.

2. Configure the following settings for *port1*, then click *Apply* to apply your changes.

Name	Displays the name of the interface.
IP Address/Netmask	The IP address and netmask associated with this interface.
IPv6 Address	The IPv6 address associated with this interface.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Service Access	Select the Fortinet services that are allowed access on this interface. These include <i>FortiGate Updates</i> and <i>Web Filtering</i> . By default all service access is enabled on port1, and disabled on port2.
Default Gateway	The default gateway associated with this interface.
Primary DNS Server	The primary DNS server IP address.
Secondary DNS Server	The secondary DNS server IP address.

To configure additional ports:

1. Go to *System Settings > Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Configure the settings as required.
4. Click *OK* to apply your changes.



The port name, default gateway, and DNS servers cannot be changed from the *Edit System Interface* pane. The port can be given an alias if needed.

Disabling ports

Ports can be disabled to prevent them from accepting network traffic

To disable a port:

1. Go to *System Settings > Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. In the *Status* field, click *Disable*
4. Click *OK* to disable the port.

Changing administrative access

Administrative access defines the protocols that can be used to connect to the FortiManager through an interface. The available options are: HTTPS, HTTP, PING, SSH, TELNET, SNMP, and Web Service.

To change administrative access:

1. Go to *System Settings > Network* and click *All Interfaces*. The interface list opens.
2. Double-click on a port, right-click on a port then select *Edit* from the pop-up menu, or select a port then click *Edit* in the toolbar. The *Edit System Interface* pane is displayed.
3. Select one or more access protocols for the interface for IPv4 and IPv6, if applicable.
4. Click *OK* to apply your changes.

Static routes

Static routes can be managed from the routing tables for IPv4 and IPv6 routes.

The routing tables can be accessed by going to *System Settings > Network* and clicking *Routing Table* and *IPv6 Routing Table*.

To add a static route:

1. From the IPv4 or IPv6 routing table, click *Create New* in the toolbar. The *Create New Network Route* pane opens.
2. Enter the destination IP address and netmask, or IPv6 prefix, and gateway in the requisite fields.
3. Select the network interface that connects to the gateway from the dropdown list.
4. Click *OK* to create the new static route.

To edit a static route:

1. From the IPv4 or IPv6 routing table: double-click on a route, right-click on a route then select *Edit* from the pop-up menu, or select a route then click *Edit* in the toolbar. The *Edit Network Route* pane opens.
2. Edit the configuration as required. The route ID cannot be changed.
3. Click *OK* to apply your changes.

To delete a static route or routes:

1. From the IPv4 or IPv6 routing table, right-click on a route then select *Delete* from the pop-up menu, or select a route or routes then click *Delete* in the toolbar.
2. Click *OK* in the confirmation dialog box to delete the selected route or routes.

RAID Management

RAID helps to divide data storage over multiple disks, providing increased data reliability. For FortiManager devices containing multiple hard disks, you can configure the RAID array for capacity, performance, and/or availability.



The *RAID Management* tree menu is only available on FortiManager devices that support RAID.

Supported RAID levels

FortiManager units with multiple hard drives can support the following RAID levels:



See the [FortiManager datasheet](#) to determine your devices supported RAID levels.

Linear RAID

A Linear RAID array combines all hard disks into one large virtual disk. The total space available in this option is the capacity of all disks used. There is very little performance change when using this RAID format. If any of the drives fails, the entire set of drives is unusable until the faulty drive is replaced. All data will be lost.

RAID 0

A RAID 0 array is also referred to as striping. The FortiManager unit writes information evenly across all hard disks. The total space available is that of all the disks in the RAID array. There is no redundancy available. If any single drive fails, the data on that drive cannot be recovered. This RAID level is beneficial because it provides better performance, since the FortiManager unit can distribute disk writing across multiple disks.

- Minimum number of drives: 2
- Data protection: No protection



RAID 0 is not recommended for mission critical environments as it is not fault-tolerant.

RAID 1

A RAID 1 array is also referred to as mirroring. The FortiManager unit writes information to one hard disk, and writes a copy (a mirror image) of all information to all other hard disks. The total disk space available is that of only one hard

disk, as the others are solely used for mirroring. This provides redundant data storage with no single point of failure. Should any of the hard disks fail, there are backup hard disks available.

- Minimum number of drives: 2
- Data protection: Single-drive failure



One write or two reads are possible per mirrored pair. RAID 1 offers redundancy of data. A rebuild is not required in the event of a drive failure. This is the simplest RAID storage design with the highest disk overhead.

RAID 1s

A RAID 1 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure the hot spare is substituted for the failed drive, integrating it into the RAID array and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 5

A RAID 5 array employs striping with a parity check. Similar to RAID 0, the FortiManager unit writes information evenly across all drives but additional parity blocks are written on the same stripes. The parity block is staggered for each stripe. The total disk space is the total number of disks in the array, minus one disk for parity storage. For example, with four hard disks, the total capacity available is actually the total for three hard disks. RAID 5 performance is typically better with reading than with writing, although performance is degraded when one disk has failed or is missing. With RAID 5, one disk can fail without the loss of data. If a drive fails, it can be replaced and the FortiManager unit will restore the data on the new disk by using reference information from the parity volume.

- Minimum number of drives: 3
- Data protection: Single-drive failure

RAID 5s

A RAID 5 with hot spare array uses one of the hard disks as a hot spare (a stand-by disk for the RAID). If a hard disk fails, within a minute of the failure, the hot spare is substituted for the failed drive, integrating it into the RAID array, and rebuilding the RAID's data. When you replace the failed hard disk, the new hard disk is used as the new hot spare. The total disk space available is the total number of disks minus two.

RAID 6

A RAID 6 array is the same as a RAID 5 array with an additional parity block. It uses block-level striping with two parity blocks distributed across all member disks.

- Minimum number of drives: 4
- Data protection: Up to two disk failures.

RAID 6s

A RAID 6 with hot spare array is the same as a RAID 5 with hot spare array with an additional parity block.

RAID 10

RAID 10 (or 1+0), includes nested RAID levels 1 and 0, or a stripe (RAID 0) of mirrors (RAID 1). The total disk space available is the total number of disks in the array (a minimum of 4) divided by 2, for example:

- 2 RAID 1 arrays of two disks each,
- 3 RAID 1 arrays of two disks each,
- 6 RAID1 arrays of two disks each.

One drive from a RAID 1 array can fail without the loss of data; however, should the other drive in the RAID 1 array fail, all data will be lost. In this situation, it is important to replace a failed drive as quickly as possible.

- Minimum number of drives: 4
- Data protection: Up to two disk failures in each sub-array.



Alternative to RAID 1 when additional performance is required.

RAID 50

RAID 50 (or 5+0) includes nested RAID levels 5 and 0, or a stripe (RAID 0) and stripe with parity (RAID 5). The total disk space available is the total number of disks minus the number of RAID 5 sub-arrays. RAID 50 provides increased performance and also ensures no data loss for the same reasons as RAID 5. One drive in each RAID 5 array can fail without the loss of data.

- Minimum number of drives: 6
- Data protection: Up to one disk failure in each sub-array.



Higher fault tolerance than RAID 5 and higher efficiency than RAID 0.



RAID 50 is only available on models with 9 or more disks. By default, two groups are used unless otherwise configured via the CLI. Use the `diagnose system raid status` CLI command to view your current RAID level, status, size, groups, and hard disk drive information.

RAID 60

A RAID 60 (6+ 0) array combines the straight, block-level striping of RAID 0 with the distributed double parity of RAID 6.

- Minimum number of drives: 8
- Data protection: Up to two disk failures in each sub-array.



High read data transaction rate, medium write data transaction rate, and slightly lower performance than RAID 50.

Configuring the RAID level



Changing the RAID level will delete all data.

To configure the RAID level:

1. Go to *System Settings > RAID Management*.
2. Click *Change* in the *RAID Level* field. The *RAID Settings* dialog box is displayed.
3. From the *RAID Level* list, select a new RAID level, then click *OK*.

The FortiManager unit reboots. Depending on the selected RAID level, it may take a significant amount of time to generate the RAID array.

Monitoring RAID status

To view the RAID status, go to *System Settings > RAID Management*. The RAID Management pane displays the RAID level, status, and disk space usage. It also shows the status, size, and model of each disk in the RAID array.



The *Alert Message Console* widget, located in *System Settings > Dashboard*, provides detailed information about RAID array failures. For more information see [Alert Messages Console widget on page 484](#).

Summary



RAID Level

Status

Disk Space Usage



Raid-10 [\[Change\]](#)

System is functioning normally.

1890GB Used/ 5442GB Free/ 7332GB Total

25% Used

Disk Management

Disk Number	Disk Status	Size(GB)	Disk Model
0	✓	1862	ST2000NM0033-9ZM175
1	✓	1862	ST2000NM0033-9ZM175
2	✓	1862	ST2000NM0033-9ZM175
3	✓	1862	ST2000NM0033-9ZM175
4	✓	1862	ST2000NM0033-9ZM175
5	✓	1862	ST2000NM0033-9ZM175
6	✓	1862	ST2000NM0033-9ZM175
7	✓	1862	ST2000NM0033-9ZM175

Summary

Shows summary information about the RAID array.

Graphic

Displays the position and status of each disk in the RAID array. Hover the cursor over each disk to view details.

RAID Level

Displays the selected RAID level.

Click *Change* to change the selected RAID level. When you change the RAID settings, all data is deleted.

Status	Displays the overall status of the RAID array.
Disk Space Usage	Displays the total size of the disk space, how much disk space is used, and how much disk space is free.
Disk Management	Shows information about each disk in the RAID array.
Disk Number	Identifies the disk number for each disk.
Disk Status	Displays the status of each disk in the RAID array. <ul style="list-style-type: none"> • <i>Ready</i>: The hard drive is functioning normally. • <i>Rebuilding</i>: The FortiManager unit is writing data to a newly added hard drive in order to restore the hard drive to an optimal state. The FortiManager unit is not fully fault tolerant until rebuilding is complete. • <i>Initializing</i>: The FortiManager unit is writing to all the hard drives in the device in order to make the array fault tolerant. • <i>Verifying</i>: The FortiManager unit is ensuring that the parity data of a redundant drive is valid. • <i>Degraded</i>: The hard drive is no longer being used by the RAID controller. • <i>Inoperable</i>: One or more drives are missing from the FortiManager unit. The drive is no longer available to the operating system. Data on an inoperable drive cannot be accessed.
Size (GB)	Displays the size, in GB, of each disk.
Disk Model	Displays the model number of each disk.

Checking RAID from command line

Use command line to check if your device uses hardware or software RAID.

To check RAID type from the command line:

1. Go to *System Settings*.
2. Click *CLI Console*.
3. Type the command `diagnose system raid status` and press *Enter*.
4. The following information is shown in the output:
 - Mega RAID - this output shows that the device uses hardware RAID.
 - Software RAID - this output shows that the device uses software RAID.

Sample command line output showing RAID:

```
[Product_Name_Model] # diagnose system raid status
Mega RAID: <-- this is hardware RAID
RAID Level: Raid-50
RAID Status: OK
RAID Size: 11175GB
Groups: 2
```

```
[Product_Name_Model] # diagnose system raid status
Software RAID: <-- this is software RAID
RAID Level: Raid-50
RAID Status: OK
RAID Size: 11175GB
Groups: 2
```

Swapping hard disks

If a hard disk on a FortiManager unit fails, it must be replaced. On FortiManager devices that support hardware RAID, the hard disk can be replaced while the unit is still running - known as hot swapping. On FortiManager units with software RAID, the device must be shutdown prior to exchanging the hard disk.

To identify which hard disk failed, read the relevant log message in the *Alert Message Console* widget. See [Alert Messages Console widget on page 484](#).



Electrostatic discharge (ESD) can damage FortiManager equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiManager chassis.



When replacing a hard disk, you need to first verify that the new disk is the same size as those supplied by Fortinet and has at least the same capacity as the old one in the FortiManager unit. Installing a smaller hard disk will affect the RAID setup and may cause data loss. Due to possible differences in sector layout between disks, the only way to guarantee that two disks have the same size is to use the same brand and model.

The size provided by the hard drive manufacturer for a given disk model is only an approximation. The exact size is determined by the number of sectors present on the disk.

To hot swap a hard disk on a device that supports hardware RAID:

1. Remove the faulty hard disk.
2. Install a new disk.

The FortiManager unit automatically adds the new disk to the current RAID array. The status appears on the console. The *RAID Management* pane displays a green checkmark icon for all disks and the *RAID Status* area displays the progress of the RAID re-synchronization/rebuild.

Adding hard disks

Some FortiManager units have space to add more hard disks to increase your storage capacity.



Fortinet recommends you use the same disks as those supplied by Fortinet. Disks of other brands will not be supported by Fortinet. For information on purchasing extra hard disks, contact your Fortinet reseller.

To add more hard disks:

1. Obtain the same disks as those supplied by Fortinet.
2. Back up the log data on the FortiManager unit.
You can also migrate the data to another FortiManager unit, if you have one. Data migration reduces system down time and the risk of data loss.
3. Install the disks in the FortiManager unit.
If your unit supports hot swapping, you can do so while the unit is running. Otherwise the unit must be shut down first. See [Unit Operation widget on page 483](#) for information.
4. Configure the RAID level. See [Configuring the RAID level on page 49](#).
5. If you backed up the log data, restore it.

Administrative Domains

Administrative domains (ADOMs) enable administrators to manage only those devices that they are specifically assigned, based on the ADOMs to which they have access. When the ADOM mode is advanced, FortiGate devices with multiple VDOMs can be divided among multiple ADOMs.

Administrator accounts can be tied to one or more ADOMs, or denied access to specific ADOMs. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. Super user administrator accounts, such as the `admin` account, can see and maintain all ADOMs and the devices within them.

When FortiAnalyzer features are enabled, each ADOM specifies how long to store and how much disk space to use for its logs. You can monitor disk utilization for each ADOM and adjust storage settings for logs as needed.

The maximum number of ADOMs you can add depends on the FortiManager system model. Please refer to the FortiManager data sheet for more information.

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by administrators with the *Super_User* profile. See [Administrators on page 73](#).



Non-FortiGate devices, except for FortiAnalyzer devices, are automatically located in specific ADOMs for their device type. They cannot be moved to other ADOMs.

One FortiAnalyzer device can be added to each ADOM. For more information, see [Adding FortiAnalyzer devices on page 119](#).

Default ADOMs

FortiManager includes default ADOMs for specific types of devices. When you add one or more of these devices to the FortiManager, the devices are automatically added to the appropriate ADOM, and the ADOM becomes selectable. When a default ADOM contains no devices, the ADOM is not selectable.

For example, when you add a FortiClient EMS device to the FortiManager, the FortiClient EMS device is automatically added to the default FortiClient ADOM. After the FortiClient ADOM contains a FortiClient EMS device, the FortiClient ADOM is selectable when you log into FortiManager or when you switch between ADOMs.

You can view all of the ADOMs, including default ADOMs without devices, on the *System Settings > All ADOMs* pane.

Organizing devices into ADOMs

You can organize devices into ADOMs to allow you to better manage these devices. Devices can be organized by whatever method you deem appropriate, for example:

- Firmware version: group all devices with the same firmware version into an ADOM.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a different region into another ADOM.
- Administrative users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.

- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

Enabling and disabling the ADOM feature

By default, ADOMs are disabled. Enabling and configuring ADOMs can only be done by super user administrators.

When ADOMs are enabled, the *Device Manager*, *Policy & Objects*, *AP Manager*, *FortiClient Manager*, and *VPN Manager* panes are displayed per ADOM. If FortiAnalyzer features are enabled, the *FortiView*, *Log View*, *Event Management*, and *Reports* panes are also displayed per ADOM. You select the ADOM you need to work in when you log into the FortiManager unit. [Switching between ADOMs on page 37](#).



ADOMs must be enabled to support FortiMail and FortiWeb logging and reporting. When a FortiMail or FortiWeb device is promoted to the DVM table, the device is added to their respective default ADOM and will be visible in the left-hand tree menu.



FortiGate and FortiCarrier devices cannot be grouped into the same ADOM. FortiCarrier devices are added to a specific default FortiCarrier ADOM.

To enable the ADOM feature:

1. Log in to the FortiManager as a super user administrator.
2. Go to *System Settings > Dashboard*.
3. In the *System Information* widget, toggle the *Administrative Domain* switch to *ON*.
You will be automatically logged out of the FortiManager and returned to the log in screen.

To disable the ADOM feature:

1. Remove all the devices from all non-root ADOMs. That is, add all devices to the root ADOM.
2. Delete all non-root ADOMs. See [Deleting ADOMs on page 61](#).
Only after removing all the non-root ADOMs can ADOMs be disabled.
3. Go to *System Settings > Dashboard*.
4. In the *System Information* widget, toggle the *Administrative Domain* switch to *OFF*.
You will be automatically logged out of the FortiManager and returned to the log in screen.



The ADOMs feature cannot be disabled if ADOMs are still configured and have managed devices in them.

ADOM device modes

An ADOM has two device modes: *Normal* (default) and *Advanced*.

In *Normal* mode, you cannot assign different FortiGate VDOMs to different ADOMs. The FortiGate unit can only be added to a single ADOM.

In *Advanced* mode, you can assign a VDOM from a single device to a different ADOM (ADOM cannot be in backup mode). This allows you to analyze data for individual VDOMs, but will result in more complicated management scenarios. It is recommended only for advanced users.

To change from *Advanced* mode back to *Normal* mode, you must ensure no FortiGate VDOMs are assigned to an ADOM.

To change the ADOM device mode:

1. Go to *System Settings > Advanced > Advanced Settings*.
2. In the ADOM Mode field, select either *Normal* or *Advanced*.
3. Select *Apply* to apply your changes.

ADOM modes

When creating an ADOM, the mode can be set to *Normal* or *Backup*.

Normal mode ADOMs

When creating an ADOM in Normal Mode, the ADOM is considered *Read/Write*, where you are able to make changes to the ADOM and managed devices from the FortiManager. FortiGate units in the ADOM will query their own configuration every 5 seconds. If there has been a configuration change, the FortiGate unit will send a diff revision on the change to the FortiManager using the FGFM protocol.

Backup mode ADOMs

When creating an ADOM in Backup Mode, the ADOM is considered *Read Only*, where you are not able to make changes to the ADOM and managed devices from the FortiManager. Changes are made via scripts which are run on the managed device, or through the device's GUI or CLI directly. Revisions are sent to the FortiManager when specific conditions are met:

- Configuration change and session timeout
- Configuration change and log out
- Configuration change and reboot
- Manual configuration backup from the managed device.

Backup mode enables you to configure an ADOM where all the devices that are added to the ADOM will only have their configuration backed up. Configuration changes cannot be made to the devices in backup ADOM. You can push any existing revisions to managed devices. You can still monitor and review the revision history for these devices, and scripting is still allowed for pushing scripts directly to FortiGate units.

Managing ADOMs

The ADOMs feature must be enabled before ADOMs can be created or configured. See [Enabling and disabling the ADOM feature on page 54](#).

To create and manage ADOMs, go to *System Settings > All ADOMs*.

+ Create New Edit Delete Enter ADOM More				
<input type="checkbox"/>	Name	Firmware Version	Central VPN	Allocated Storage
▼ Central Management (4)				
<input type="checkbox"/>	ADOM-2	FortiGate 5.4	✗	1000.0 MB
<input type="checkbox"/>	FortiCarrier	FortiCarrier 5.4	✗	1000.0 MB
<input type="checkbox"/>	root	FortiGate 5.4	✓	1000.0 MB
<input type="checkbox"/>	Global Database	Global 5.4	✗	-
▼ Backup Mode (1)				
<input type="checkbox"/>	FG52	FortiGate 5.2	✓	1000.0 MB
▼ Other Device Types (11)				
<input type="checkbox"/>	FortiAnalyzer	FortiAnalyzer	✗	1000.0 MB
<input type="checkbox"/>	FortiAuthenticator	FortiAuthenticator	✗	1000.0 MB
<input type="checkbox"/>	FortiCache	FortiCache	✗	1000.0 MB
<input type="checkbox"/>	FortiClient	FortiClient	✗	1000.0 MB
<input type="checkbox"/>	FortiDDoS	FortiDDoS	✗	1000.0 MB
<input type="checkbox"/>	FortiMail	FortiMail	✗	1000.0 MB
<input type="checkbox"/>	FortiManager	FortiManager	✗	1000.0 MB
<input type="checkbox"/>	FortiSandbox	FortiSandbox	✗	1000.0 MB
<input type="checkbox"/>	FortiWeb	FortiWeb	✗	1000.0 MB
<input type="checkbox"/>	Syslog	Syslog	✗	1000.0 MB
<input type="checkbox"/>	Chassis	-	✗	-

Create New

Create a new ADOM. See [Creating ADOMs on page 57](#).

Edit

Edit the selected ADOM. This option is also available from the right-click menu. See [Editing an ADOM on page 60](#).

Delete

Delete the selected ADOM or ADOMs. You cannot delete default ADOMs. This option is also available from the right-click menu. See [Deleting ADOMs on page 61](#).

Enter ADOM

Switch to the selected ADOM. This option is also available from the right-click menu.

More

Select *Expand Devices* to expand all of the ADOMs to show the devices in each ADOM. Select *Collapse Devices* to collapse the device lists. Select *Upgrade* to upgrade the ADOM; see [ADOM versions on page 61](#). These options are also available from the right-click menu.

Search

Enter a search term to search the ADOM list.

Name

The name of the ADOM.
ADOMs are listed in the following groups: *Central Management*, *Backup Mode* (if there are any backup mode ADOMs), and *Other Device Types*. A group can be collapsed or expanded by clicking the triangle next to its name.

Firmware Version

The firmware version of the ADOM. Devices in the ADOM should have the same firmware version.
See [ADOM versions on page 61](#) for more information.

Central VPN	Whether or not central VPN management is enabled for the ADOM.
Allocated Storage	The amount of hard drive storage space allocated to the ADOM.
Devices	The number of devices and VDOMs that the ADOM contains. The device list can be expanded or by clicking the triangle.

Creating ADOMs

To create a new ADOM, you must be logged in as a super user administrator.

Consider the following when creating ADOMs:

- The maximum number of ADOMs that can be created depends on the FortiManager model. For more information, see the FortiManager data sheet at <https://www.fortinet.com/products/management/fortimanager.html>.
- You must use an administrator account that is assigned the *Super_User* administrative profile.
- You can add a device to only one ADOM. You cannot add a device to multiple ADOMs.
- You cannot add FortiGate and FortiCarrier devices to the same ADOM. FortiCarrier devices are added to a specific, default FortiCarrier ADOM.
- You can add one or more VDOMs from a FortiGate device to one ADOM. If you want to add individual VDOMs from a FortiGate device to different ADOMs, you must first enable advanced device mode. See [ADOM device modes on page 55](#).
- When FortiAnalyzer features are enabled, you can configure how an ADOM handles log files from its devices. For example, you can configure how much disk space an ADOM can use for logs, and then monitor how much of the allotted disk space is used. You can also specify how long to keep logs indexed in the SQL database and how long to keep logs stored in a compressed format.

To create an ADOM

1. Ensure that ADOMs are enabled. See [Enabling and disabling the ADOM feature on page 54](#).
2. Go to *System Settings > All ADOMs*.
3. Click *Create New* in the toolbar. The *Create New ADOM* pane is displayed.

Create New ADOM

Name:

Type: FortiGate 5.6 5.4 5.2

Devices: + Select Device

Name	IP Address	Platform
Click to select devices for this ADOM.		

Central Management: ☐ VPN ☐ SD-WAN ☒ FortiAP

Mode: ☒ Normal ☐ Backup

Default Device Selection for Install: ☒ Select All ☐ Unselect All

Data Policy

Keep Logs for Analytics: Days

Keep Logs for Archive: Days

Disk Utilization

Maximum Allowed: MB Out of Available: 0.0 KB

Analytics : Archive: 30% ☐ Modify

Alert and Delete When Usage Reaches:

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

4. Configure the following settings, then click *OK* to create the ADOM.

Name	Type a name that allows you to distinguish this ADOM from your other ADOMs. ADOM names must be unique.
Type	Select either FortiGate or FortiCarrier from the dropdown menu. The ADOM type cannot be edited. Other device types are added to their respective default ADOM when registering with FortiManager.
Version	Select the version of the devices in the ADOM. The ADOM version cannot be edited.
Devices	Add a device or devices with the selected versions to the ADOM. The search field can be used to find specific devices. See Assigning devices to an ADOM on page 59 .
Central Management	Select the <i>VPN</i> checkbox to enable central VPN management. Select the <i>SD-WAN</i> checkbox to enable central WAN link balancing. Select the <i>FortiAP</i> checkbox to enable central FortiAP management. This checkbox is selected by default. This option is only available when the <i>Mode</i> is <i>Normal</i> .
Mode	Select <i>Normal</i> mode if you want to manage and configure the connected FortiGate devices from the FortiManager GUI. Select <i>Backup</i> mode if you want to backup the FortiGate configurations to the FortiManager, but configure each FortiGate locally. See ADOM modes on page 55 for more information.
Default Device Selection for Install	Select either <i>Select All</i> or <i>Unselect All</i> . This option is only available when the <i>Mode</i> is <i>Normal</i> .
Data Policy	Specify how long to keep logs in the indexed and compressed states. This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 390 .
Keep Logs for Analytics	Specify how long to keep logs in the indexed state. During the indexed state, logs are indexed in the SQL database for the specified amount of time. Information about the logs can be viewed in the <i>FortiView</i> , <i>Event Management</i> , and <i>Reports</i> modules. After the specified length of time expires, Analytics logs are automatically purged from the SQL database.
Keep Logs for Archive	Specify how long to keep logs in the compressed state. During the compressed state, logs are stored in a compressed format on the FortiManager unit. When logs are in the compressed state, information about the log messages cannot be viewed in the <i>FortiView</i> , <i>Event Management</i> , or <i>Reports</i> modules. After the specified length of time expires, Archive logs are automatically deleted from the FortiManager unit.

Disk Utilization	Specify how much disk space to use for logs. This section is only available when FortiAnalyzer features are enabled. See FortiAnalyzer Features on page 390 .
Maximum Allowed	Specify the maximum amount of FortiManager disk space to use for logs, and select the unit of measure. The total available space on the FortiManager unit is shown. For more info about the maximum available space for each FortiManager unit, see Disk space allocation on page 205 .
Analytics : Archive	Specify the percentage of the allotted space to use for Analytics and Archive logs. Analytics logs require more space than Archive logs. For example, a setting of 70% and 30% indicates that 70% of the allotted disk space will be used for Analytics logs, and 30% of the allotted space will be used for Archive logs. Select the <i>Modify</i> checkbox to change the setting.
Alert and Delete When Usage Reaches	Specify at what data usage percentage an alert messages will be generated and logs will be automatically deleted. The oldest Archive log files or Analytics database tables are deleted first.

Assigning devices to an ADOM

To assign devices to an ADOM you must be logged in as a super user administrator. Devices cannot be assigned to multiple ADOMs.

To assign devices to an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the devices that you want to add to the ADOM. Only devices with the same version as the ADOM can be added. The selected devices are displayed in the *Devices* list.
If the ADOM mode is *Advanced* you can add separate VDOMs to the ADOM as well as units.
5. When done selecting devices, click *Close* to close the *Select Device* list.
6. Click *OK*.

The selected devices are removed from their previous ADOM and added to this one.

Assigning VDOMs to an ADOM

To assign VDOMs to an ADOM you must be logged in as a super user administrator and the ADOM mode must be *Advanced* (see [ADOM device modes on page 55](#)). VDOMs cannot be assigned to multiple ADOMs.

To assign VDOMs to an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select the *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Click *Select Device*. The *Select Device* list opens on the right side of the screen.
4. Select the VDOMs that you want to add to the ADOM. Only VDOMs on devices with the same version as the ADOM can be added. The selected VDOMs are displayed in the *Devices* list.
5. When done selecting VDOMs, click *Close* to close the *Select Device* list.
6. Click *OK*.

The selected VDOMs are removed from their previous ADOM and added to this one.

Assigning administrators to an ADOM

Super user administrators can create other administrators and either assign ADOMs to their account or exclude them from specific ADOMs, constraining them to configurations and data that apply only to devices in the ADOMs they can access.



By default, when ADOMs are enabled, existing administrator accounts other than *admin* are assigned to the *root* domain, which contains all devices in the device list. For more information about creating other ADOMs, see [Creating ADOMs on page 57](#).

To assign an administrator to specific ADOMs:

1. Log in as a super user administrator. Other types of administrators cannot configure administrator accounts when ADOMs are enabled.
2. Go to *System Settings > Admin > Administrator*.
3. Double-click on an administrator, right-click on an administrator and then select the *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
4. Edit the *Administrative Domain* field as required, either assigning or excluding specific ADOMs.
5. Select *OK* to apply your changes.



The *admin* administrator account cannot be restricted to specific ADOMs.

Editing an ADOM

To edit an ADOM you must be logged in as a super user administrator. The ADOM type and version cannot be edited. For the default ADOMs, the name cannot be edited.

To edit an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit ADOM* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting ADOMs

To delete an ADOM, you must be logged in as a super-user administrator (see [Administrator profiles on page 85](#)), such as the *admin* administrator.

Prior to deleting an ADOM:

- All devices must be removed from the ADOM. Devices can be moved to another ADOM, or to the root ADOM. See [Assigning devices to an ADOM on page 59](#).
- Global policy packages assigned to the ADOM must be unassigned. See [Assign a global policy package on page 220](#).
- References to the ADOM must be removed from administrator accounts (or the accounts deleted). See [Assigning administrators to an ADOM on page 60](#).

To delete an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Ensure that the ADOM or ADOMs being deleted have no devices in them.
3. Select the ADOM or ADOMs you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation box to delete the ADOM or ADOMs.



Default ADOMs cannot be deleted.

ADOM versions

ADOMs can concurrently manage FortiGate units running FortiOS 5.2, 5.4, and 5.6, allowing devices running these versions to share a common database. This allows you to continue to manage an ADOM as normal while upgrading the devices within that ADOM.

When adding a new FortiGate unit to an ADOM, the FortiGate unit should have the same FortiOS version as the ADOM.



This feature can be used to facilitate upgrading to new firmware.

Importing policies from devices running higher versions than the ADOM is not supported.
Installation to devices running higher versions is supported.



FortiManager 5.6 supports FortiOS 5.2, 5.4, and 5.6 ADOMs. For a complete list of supported devices and firmware versions, see the FortiManager Release Notes.

Each ADOM is associated with a specific FortiOS version, based on the firmware version of the devices that are in that ADOM. This version is selected when creating a new ADOM (see [Creating ADOMs on page 57](#)), and can be updated only after all of the devices within the ADOM have been updated to the same FortiOS firmware version.

The general steps for upgrading an ADOM containing multiple devices running FortiOS 5.4 from 5.4 to 5.6 are as follows:

1. In the ADOM, upgrade one of the FortiGate units to FortiOS 5.6, and then resynchronize the device. See [Firmware on page 151](#) for more information.
All of the ADOM objects, including Policy Packages, remain as 5.4 objects.
 2. Upgrade the rest of the FortiGate units in the ADOM to FortiOS 5.6.
 3. Upgrade the ADOM to 5.6. See [Upgrading an ADOM on page 64](#) for more information.
All of the database objects will be converted to 5.6 format, and the GUI content for the ADOM will change to reflect 5.6 features and behavior.
-



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded.

Global database version

The global database is reset when the database version is edited. The database is not reset when the global database ADOM is upgraded using the *Upgrade* command.



The global database ADOM should only be upgraded after all the ADOMs that are using a global policy package have been upgraded.

To upgrade the global database ADOM:

1. Go to *System Settings > All ADOMs*.
2. Select *Global Database* then click *More > Upgrade* in the toolbar, or right-click *Global Database* and select *Upgrade*.
If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Click *OK* in the *Upgrade ADOM* dialog box.
4. After the upgrade finishes, click *Close* to close the dialog box.

To edit the global database version:

Editing the global database version will reset the database. All global policy packages will be lost. This should only be used when starting to use the global database for the first time, or when resetting the database is required.

1. Go to *System Settings > All ADOMs*.
2. Select *Global Database* then click *Edit* in the toolbar, or right-click *Global Database* and select *Edit*. The *Edit Global Database* window opens.
3. Select the version.
4. Click *OK* to save the setting.
5. A confirmation dialog box will be displayed. Click *OK* to continue.

Concurrent ADOM access

Concurrent ADOM access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function must be enabled.

When workspace mode is enabled, concurrent ADOM access is disabled. An administrator must lock the ADOM before they can make device-level changes to it, and only one administrator can hold the lock at a time, while other administrators have read-only access. Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that is locked by another administrator. See [Locking an ADOM on page 64](#).

When workspace is disabled, concurrent ADOM access is enabled, and multiple administrators can log in and make changes to the same ADOM at the same time.

To enable workspace mode, and disable concurrent ADOM access:

1. Enter the following CLI commands:

```
config system global
    set workspace-mode normal
end
```

To disable workspace mode, and enable concurrent ADOM access:

1. Enter the following CLI commands:

```
config system global
    set workspace-mode disabled
Warning: disabling workspaces may cause some logged in users to lose their unsaved data.
Do you want to continue? (y/n) y
end
```



After changing the workflow mode, your session will end and you will be required to log back in to the FortiManager.

Locking an ADOM

If workspace is enabled, you must lock an ADOM prior to performing device-level changes to it. If you are making changes at the ADOM level, you can leave the ADOM unlocked and lock policy packages or objects independently.

The padlock icon, shown next to the ADOM name on the banner and in the *All ADOMs* list, will turn from gray to green when you lock an ADOM. If it is red, it means that another administrator has locked the ADOM.

Optionally, ADOM lock override can be enabled, allowing an administrator to unlock an ADOM that has been locked by another administrator and discard all of their unsaved changes.

To lock an ADOM:

- Ensure that you are in the specific ADOM that you will be editing (top right corner of the GUI), then select *Lock* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Lock* from the right-click menu.

The ADOM will now be locked, allowing you to make changes to it and preventing other administrators from making changes unless lock override is enabled. The lock icon will turn into a green locked padlock.

To unlock an ADOM:

- Ensure you have saved any changes you may have made to the ADOM then select *Unlock ADOM* from the banner.
- Or, go to *System Settings > All ADOMs*, right-click on an ADOM, and select *Unlock* from the right-click menu.

If there are unsaved changes to the ADOM, a dialog box will give you the option of saving or discarding your changes before unlocking the ADOM. The ADOM will now be unlocked, allowing any administrator to lock the ADOM and make changes.

To enable or disable ADOM lock override:

Enter the following CLI commands:

```
config system global
  set lock-preempt {enable | disable}
end
```

Upgrading an ADOM

To upgrade an ADOM, you must be logged in as a super user administrator.



An ADOM can only be upgraded after all the devices within the ADOM have been upgraded. See [ADOM versions on page 61](#) for more information.

To upgrade an ADOM:

1. Go to *System Settings > All ADOMs*.
2. Right-click on an ADOM and select *Upgrade*, or select an ADOM and then select *More > Upgrade* from the toolbar. If the ADOM has already been upgraded to the latest version, this option will not be available.
3. Select *OK* in the confirmation dialog box to upgrade the device.
If all of the devices within the ADOM are not already upgraded, the upgrade will be aborted and an error message will be shown. Upgrade the remaining devices within the ADOM, then return to step 1 to try upgrading the ADOM again.

Workflow Mode

Workflow mode is used to control the creation, configuration, and installation of policies and objects. It helps to ensure all changes are reviewed and approved before they are applied.

When workflow mode is enabled, the ADOM must be locked and a session must be started before policy or object changes can be made in an ADOM. Workflow approvals must be configured for an ADOM before any sessions can be started in it.

Once the required changes have been made, the session can either be discarded and the changes deleted, or it can be submitted for approval. The session can also be saved and continued later, but no new sessions can be created until the saved session has been submitted or discarded.

When a session is submitted for approval, email messages are sent to the approvers, who can then approve or reject the changes directly from the email message. Sessions can also be approved or rejected by the approvers from within the ADOM itself.



Sessions must be approved in the order they were created.

If one approver from each approval group approves the changes, then another email message is sent, and the changes are implemented. If any of the approvers reject the changes, then the session can be repaired and resubmitted as a new session, or discarded. When a session is discarded, all later sessions are also discarded. After multiple sessions have been approved, a previous session can be reverted to, undoing all the later sessions.

The changes made in a session can be viewed at any time from the session list in the ADOM by selecting *View Diff*. The ADOM does not have to be locked to view the differences.

Enable or disable workflow mode

Workflow mode can only be enabled or disabled from the CLI.



After changing the workflow mode, your session will end, and you will be required to log back in to the FortiManager.

To enable or disable workflow mode:

1. Go to *System Settings > Dashboard*.
2. In the CLI Console widget enter the following CLI commands in their entirety:

```
config system global
  set workspace-mode {workflow | disable}
end
```



When `workspace-mode` is `workflow`, *Device Manager* and *Policy & Objects* are read-only. You must lock the ADOM to create a new workflow session.

Workflow approval

Workflow approval matrices specify which users must approve or reject policy changes for each ADOM.

Up to eight approval groups can be added to an approval matrix. One user from each approval group must approve the changes before they are accepted. An approval email will automatically be sent to each member of each approval group when a change request is made.

Email notifications are automatically sent to each approver, as well as other administrators as required. A mail server must be configured, see [Mail Server on page 518](#), and each administrator must have a contact email address configured, see [Managing administrator accounts on page 74](#).



This menu is only available when `workspace-mode` is set to `workflow`.

To create a new approval matrix:

1. Go to *System Settings > Admin > Approval Matrix*.
2. Click *Create New*.

New Approval Matrix

ADOM	fgt54-2	
Approval Group # 1	<div style="border: 1px solid #ccc; padding: 2px;"> x TLeela x PJFry </div>	-
Approval Group # 2	<div style="border: 1px solid #ccc; padding: 2px;"> x BBRodriguez x HConrad </div>	+ -
Send an Email Notification to	<div style="border: 1px solid #ccc; padding: 2px;"> x admin </div>	
Mail Server	localMail	

OK
Cancel

3. Configure the following settings:

ADOM	Select the ADOM from the dropdown list.
Approval Group	Select to add approvers to the approval group. Select the add icon to create a new approval group. Select the delete icon to remove an approval group. At least one approver from each group must approve the change for it to be adopted.
Send an Email Notification to	Select to add administrators to send email notifications to.
Mail Server	Select the mail server from the dropdown list. A mail server must already be configured. See Mail Server on page 518 .

4. Click *OK* to create the approval matrix.

Workflow sessions

Administrators use workflow sessions to make changes to policies and objects. The session is then submitted for review and approval or rejection by the administrators defined in the ADOMs workflow approval matrix.

Administrators with the appropriate permissions will be able to approve or reject any pending requests. When viewing the session list, they can choose any pending sessions, and click the approve or reject buttons. They can also add a comment to the response. A notification will then be sent to the administrator that submitted the session and all of the approvers.



You cannot prevent administrators from approving their own workflow sessions.

If the session was approved, no further action is required. If the session was rejected, the administrator will need to either repair or discard the session.

The Global Database ADOM includes the *Assignment* option, for assigning the global policy package to an ADOM. Assignments can only be created and edited when a session is in progress. After a global database session is approved, the policy package can be assigned to the configured ADOM. A new session will be created on the assigned ADOM and automatically submitted; it must be approved for the changes to take effect.

A session can be discarded at any time before it is approved.

After multiple sessions have been submitted or approved, a previously approved session can be reverted to, undoing all the later sessions. This creates a new session at the top of the session list that is automatically submitted for approval.



A workflow approval matrix must be configured for the ADOM to which the session applies before a workflow session can be started. See [Workflow approval on page 66](#).

Starting a workflow session

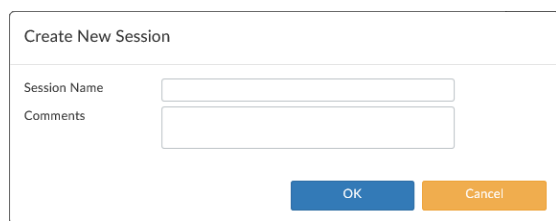
A workflow session must be started before changes can be made to the policies and objects. A session can be saved and continued at a later time, discarded, or submitted for approval.



While a session is in progress, devices cannot be added or installed.

To start a workflow session:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. Click *Lock* in the banner. The padlock icon changes to a locked state and the ADOM is locked.
4. From the *Sessions* menu, select *Session List*. The *Session List* dialog box opens; see [The session list on page 71](#).
5. Click *Create New Session*.



6. Enter a name for session, add a comment describing the session, then click *OK* to start the session. You can now make the required changes to the policy packages and objects. See [Policy & Objects on page 212](#).

Saved sessions

A session can be saved and continued later.



A new session cannot be started until the in-progress or saved session has either been submitted for approval or discarded.

To save your session:

While currently working in a session, click *Save* in the toolbar. After saving the session, the ADOM will remain locked, and you can continue to edit it.

To continue a saved session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens.
4. Click *Continue Session In Progress* to continue the session.

Discarding a session

A session can be discarded at any time before it is approved. A session cannot be recovered after it is discarded.



When a session is discarded, all sessions after it in the session list will also be discarded.

To discard an in-progress session:

1. Select *Session > Discard*.
2. Enter comments in the *Discard Session* dialog box.
3. Click *OK*. The changes are deleted and the session is discarded.

To discard saved, submitted, or rejected sessions:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens.
4. Select the session that is to be discarded, then click *Discard*.
5. Select *OK* in the *Discard Session* pop-up.

Submitting a session

When all the required changes have been made, the session can be submitted for approval. A session must be open to be submitted for approval.

When the session is submitted, email messages are sent to all of the approvers and other administrators defined in the approval matrix (see [Workflow approval on page 66](#)), and the ADOM is automatically unlocked.

To submit a session for approval:

1. Select *Sessions > Submit*.
2. Enter the following in the *Submit for Approval* dialog box:

Comments	Enter a comment describing the changes that have been made in this session.
Attach configuration change details	Select to attach configuration change details to the email message.

3. Click *OK* to submit the session.

Approving or rejecting a session

Sessions can be approved or rejected by the members of the approval groups either directly from the email message that is generated when the session is submitted, or from the session list. A session that has been rejected must be repaired or discarded before the next session can be approved.

When a session is approved or rejected, new email messages are sent out.

To approve or reject a session from the email message:

1. If the configuration changes HTML file is attached to the email message, open the file to review the changes.
2. Select *Approve this request* or *Reject this request* to approve or reject the request. You can also Select *Login FortiManager to process this request* to log in to the FortiManager and approve or reject the session from the session list.
A web page will open showing the basic information, approval matrix, and session log for the session, highlighting if the session was approved or rejected. A new email message will also be sent containing the same information.
3. On the last line of the session log on the web page, select *Click here to add comments* to add a comment about why the session was approved or rejected.

To approve a session from the session list:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens; see [The session list on page 71](#).
4. Select a session that can be approved from the list.
5. Optionally, click *View Diff* to view the changes that you are approving.
6. Click *Approve*.
7. Enter a comment in the *Approve Session* pop-up, then click *OK* to approve the session.

To reject a session from the session list:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens; see [The session list on page 71](#).
4. Select a session that can be rejected from the list.
5. Optionally, click *View Diff* to view the changes that you are rejecting.
6. Click *Reject*.
7. Enter a comment in the *Reject Session* pop-up, then click *OK* to reject the session.

Repairing a rejected session

When a session is rejected, it can be repaired to correct the problems with it.

To repair a workflow session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens; see [The session list on page 71](#).
4. Select a rejected session, then click *Repair*.
A new session is created and started, with the changes from the rejected session, so it can be corrected.

Reverting a session

A session can be reverted to after other sessions have been submitted or approved. If this session is approved, it will undo all the changes made by later sessions, though those sessions must be approved before the reverting session can be approved. You can still revert to any of those sessions without losing their changes.

When a session is reverted, a new session is created and automatically submitted for approval.

To revert a session:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects* and lock the ADOM.
3. Go to *Sessions > Session List*. The *Session List* dialog box opens; see [The session list on page 71](#).
4. Select the session, then click *Revert*.

The session list

To view the session list, In *Policy & Objects*, go to *Sessions > Session List*. Different options will be available depending on the various states of the sessions (in progress, approved, etc.). When an ADOM is unlocked, only the comments and *View Diff* command are available.

Session List

☒ Approve
 ☒ Reject
 ☒ Discard
 ☒ View Diff

ID	Name	User	Date Submi...	Approved/...	Comments
3	Session-...	admin		0/1	It didn't wor...
2	Session-...	HConrad	2016-04-19...	0/1	bureaucrati...
1	Session-9	admin	2016-04-19...	0/1	This is a test...

+ Add Comment

[HConrad] - 2016-04-19 05:53:08
 bureaucratic stuff
 [HConrad] - 2016-04-19 12:52:46
 bureaucratic stuff

Continue Session In Progress
 Continue Without Session

The following options and information are available:

Approve	Approve the selected session. Enter comments in the <i>Approve Session</i> dialog box as required.
Reject	Reject the selected session. Enter comments in the <i>Reject Session</i> dialog box as required. A rejected session must be repaired before the next session in the list can be approved.
Discard	Discard the selected session. If a session is discarded, all later sessions are also discarded.

Repair	Repair the selected rejected session. A new session will be created and added to the top of the session list with the changes from the rejected session so they can be repaired as needed.
Revert	Revert back to the selected session, undoing all the changes made by later sessions. A new session will be created, added to the top of the session list, and automatically submitted for approval.
View Diff	View the changes that were made prior to approving or rejecting the session. Select details to view specific changes within a policy package.
ID	A unique number to identify the session.
Name	The user-defined name to identify the session. The icon shows the status of the session: waiting for approval, approved, rejected, repaired, or in progress. Hover the cursor over the icon to see a description.
User	The administrator who created the session.
Date Submitted	The date and time the session was submitted for approval.
Approved/...	The number of approval groups that have approved the session out of the number of groups that have to approve the session. Hover the cursor over the table cell to view the group members.
Comments	The comments for the session. All the comments are shown on the right of the dialog box for the selected session. Session approvers can also add comments to the selected session without having to approve or reject the session.
Create New Session	Select to create a new workflow session. This option is not available when a session has been saved or is already in progress.
Continue Session in Progress	Select to continue a session that was previously saved or is already in progress. This option is only available when a session is in progress or saved.
Continue Without Session	Select to continue without starting a new session. When a new session is not started, all policy and objects are read-only.

Administrators

The *System Settings > Admin* menu enables you to configure administrator accounts, access profiles, remote authentication servers, and adjust global administrative settings for the FortiManager unit.

Administrator accounts are used to control access to the FortiManager unit. Local and remote authentication is supported, as well as two-factor authentication. Administrator profiles define different types of administrators and the level of access they have to the FortiManager unit, as well as the devices registered to it.

Global administration settings, such as the GUI language and password policies, can be configured on the *Admin Settings* pane. See [Global administration settings on page 98](#) for more information.

In workflow mode, approval matrices can be create and managed on the *Approval Matrix* pane. See [Workflow approval on page 66](#) for more information.

Trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative permissions. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiManager unit does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply to both the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.



If you set trusted hosts and want to use the Console Access feature of the GUI, you must also set 127.0.0.1/255.255.255.255 as a trusted host.

Monitoring administrators

The *Admin Session List* lets you view a list of administrators currently logged in to the FortiManager unit.

To view logged in administrators:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.

The following information is available:

User Name	The name of the administrator account. Your session is indicated by <i>(current)</i> .
IP Address	The IP address where the administrator is logging in from. This field also displays the logon type (GUI, jsconsole, SSH, or telnet).
Start Time	The date and time the administrator logged in.
Time Out (mins)	The maximum duration of the session in minutes (1 to 480 minutes).

Disconnecting administrators

Administrators can be disconnected from the FortiManager unit from the *Admin Session List*.

To disconnect administrators:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *Current Administrators* field, click the *Current Session List* button. The *Admin Session List* opens in the widget.
3. Select the administrator or administrators you need to disconnect.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.

The selected administrators will be automatically disconnected from the FortiManager device.

Managing administrator accounts

Go to *System Settings > Admin > Administrator* to view the list of administrators and manage administrator accounts.

Only administrators with the *Super_User* profile can see the complete administrators list. If you do not have certain viewing permissions, you will not see the administrator list. When ADOMs are enabled, administrators can only access the ADOMs they have permission to access.

+ Create New Edit Delete Column Settings Table View						
<input type="checkbox"/>	User Name	Type	Profile	ADOMs	Policy Packages	Trusted IPv4 Hosts
<input type="checkbox"/>	123	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0
<input type="checkbox"/>	Fry	RADIUS	Standard_User	ADOM-2	ADOM-2:default	0.0.0.0/0.0.0.0
<input type="checkbox"/>	PKIup	PKI	Restricted_User	FG52 FortiClient FortiAuthenticator FortiCarrier	All Packages	0.0.0.0/0.0.0.0
<input type="checkbox"/>	Restored	Restricted Admin LOCAL	RatedR	FG52	All Packages	0.0.0.0/0.0.0.0
<input type="checkbox"/>	T1	TACACS+	Restricted_User	Exclude: FG52 ADOM-2	All Packages	0.0.0.0/0.0.0.0
<input type="checkbox"/>	Tape2	LDAP	Package_User	root Syslog FCRCRD	FCRCRD:default FortiCarrier:default root:default	0.0.0.0/0.0.0.0
<input type="checkbox"/>	admin	LOCAL	Super_User	All ADOMs	All Packages	0.0.0.0/0.0.0.0

The following options are available:

Create New	Create a new administrator. See Creating administrators on page 75 .
Edit	Edit the selected administrator. See Editing administrators on page 78 .

Delete	Delete the selected administrator or administrators. See Deleting administrators on page 78 .
Column Settings	Change the displayed columns.
Table View/Tile View	Change the view of the administrator list. Table view shows a list of the administrators in a table format. Tile view shows a separate card for each administrator in a grid pattern.
Search	Search the administrators.
Change Password	Change the selected administrator's password. This option is only available from the right-click menu. See Editing administrators on page 78 .

The following information is shown:

User Name	The name the administrator uses to log in.
Type	The user type, as well as if the administrator uses a wildcard.
Profile	The profile applied to the administrator. See Administrator profiles on page 85
ADOMs	The ADOMs the administrator has access to or is excluded from.
Policy Packages	The policy packages the administrator can access.
Comments	Comments about the administrator account. This column is hidden by default.
Email	The contact email associated with the administrator. This column is hidden by default.
Phone	The contact phone number associated with the administrator. This column is hidden by default.
Trusted IPv4 Hosts	The IPv4 trusted host(s) associated with the administrator. See Trusted hosts on page 73 .
Trusted IPv6 Hosts	The IPv6 trusted host(s) associated with the administrator. See Trusted hosts on page 73 . This column is hidden by default.

Creating administrators

To create a new administrator account, you must be logged in to an account with sufficient privileges, or as a super user administrator.

You need the following information to create an account:

- Which authentication method the administrator will use to log in to the FortiManager unit. Local, remote, and Public Key Infrastructure (PKI) authentication methods are supported.
- What administrator profile the account will be assigned, or what system privileges the account requires.
- If ADOMs are enabled, which ADOMs the administrator will require access to.
- If using trusted hosts, the trusted host addresses and network masks.



For remote or PKI authentication, the authentication must be configured before you create the administrator. See [Authentication on page 91](#) for details.

To create a new administrator:

1. Go to *System Settings > Admin > Administrators*.
2. Click *Create New* in the toolbar. The *New Administrator* pane opens.

3. Configure the following settings, and then click *OK* to create the new administrator.

User Name	Enter the name the administrator will use to log in.
Avatar	<p>Apply a custom image to the administrator.</p> <p>Click <i>Add Photo</i> to select an image already loaded to the FortiManager, or to load a new image from the management computer.</p> <p>If no image is selected, the avatar will use the first letter of the user name.</p>
Comments	Optionally, enter a description of the administrator, such as their role, location, or the reason for their account.
Admin Type	Select the type of authentication the administrator will use when logging into the FortiManager unit. One of: <i>LOCAL</i> , <i>RADIUS</i> , <i>LDAP</i> , <i>TACACS+</i> , <i>PKI</i> , or <i>Group</i> . See Authentication on page 91 for more information.
Server or Group	<p>Select the RADIUS server, LDAP server, TACACS+ server, or group, as required.</p> <p>The server must be configured prior to creating the new administrator.</p> <p>This option is not available if the <i>Admin Type</i> is <i>LOCAL</i> or <i>PKI</i>.</p>
Wildcard	<p>Select this option to set the password as a wildcard.</p> <p>This option is not available if the <i>Admin Type</i> is <i>LOCAL</i> or <i>PKI</i>.</p>
Subject	<p>Enter a comment for the PKI administrator.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>

CA	<p>Select the CA certificate from the dropdown list.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>
Required two-factor authentication	<p>Select to enable two-factor authentication.</p> <p>This option is only available if the <i>Admin Type</i> is <i>PKI</i>.</p>
New Password	<p>Enter the password.</p> <p>This option is not available if <i>Wildcard</i> is selected.</p> <p>If the <i>Admin Type</i> is <i>PKI</i>, this option is only available when <i>Require two-factor authentication</i> is selected.</p> <p>If the <i>Admin Type</i> is <i>RADIUS</i>, <i>LDAP</i>, or <i>TACACS+</i>, the password is only used when the remote server is unreachable.</p>
Confirm Password	<p>Enter the password again to confirm it.</p> <p>This option is not available if <i>Wildcard</i> is selected.</p> <p>If the <i>Admin Type</i> is <i>PKI</i>, this option is only available when <i>Require two-factor authentication</i> is selected.</p>
Admin Profile	<p>Select an administrator profile from the list. The profile selected determines the administrator's access to the FortiManager unit's features. See Administrator profiles on page 85.</p>
Administrative Domain	<p>Choose the ADOMs this administrator will be able to access.</p> <ul style="list-style-type: none"> • <i>All ADOMs</i>: The administrator can access all the ADOMs. • <i>All ADOMs except specified ones</i>: The administrator cannot access the selected ADOMs. • <i>Specify</i>: The administrator can access the selected ADOMs. <p>If the <i>Admin Profile</i> is <i>Super_User</i>, then the setting is <i>All ADOMs</i>.</p> <p>This field is available only if ADOMs are enabled. See Administrative Domains on page 53.</p>
Policy Package Access	<p>Choose the policy packages this administrator will have access to.</p> <ul style="list-style-type: none"> • <i>All Packages</i>: The administrator can access all the packages. • <i>Specify</i>: The administrator can access the selected packages. <p>This option is only available when the <i>Admin Profile</i> is not a <i>Restricted Admin</i> profile. See Restricted administrators on page 79.</p>
Web Filter Profile	<p>Select the web filter profiles that the restricted administrator will be able to edit.</p> <p>This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 261.</p>
IPS Sensor	<p>Select the IPS profiles that the restricted administrator will be able to edit.</p> <p>This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 261.</p>

Application Sensor	<p>Select the application control profiles that the restricted administrator will be able to edit.</p> <p>This option is only available when the <i>Admin Profile</i> is set to a <i>Restricted Admin</i> profile. Security profiles can be configured by going to <i>Policy & Objects > Object Configuration</i>. See Managing objects and dynamic objects on page 261.</p>
Trusted Hosts	<p>Optionally, turn on trusted hosts, then enter their IP addresses and netmasks. Up to ten IPv4 and ten IPv6 hosts can be added.</p> <p>See Trusted hosts on page 73 for more information.</p>
Meta Fields	<p>Optionally, enter the new administrator's email address and phone number.</p> <p>The email address is also used for workflow session approval notifications, if enabled. See Workflow Mode on page 65.</p>

Editing administrators

To edit an administrator, you must be logged in as a super user administrator. The administrator's name cannot be edited. An administrator's password can be changed using the right-click menu, if the password is not a wildcard.

To edit an administrator:

1. Go to *System Settings > Admin > Administrators*.
2. Double-click on an administrator, right-click on an administrator and then select *Edit* from the menu, or select the administrator then click *Edit* in the toolbar. The *Edit Administrator* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

To change an administrator's password:

1. Go to *System Settings > Admin > Administrators*.
2. Right-click on an administrator and select *Change Password* from the menu. The *Change Password* dialog box opens.
3. If you are editing the *admin* administrator's password, enter the old password in the *Old Password* field.
4. Enter the new password for the administrator in the *New Password* and *Confirm Password* fields.
5. Select *OK* to change the administrator's password.



The current administrator's password can also be changed from the admin menu in the GUI banner. See [GUI on page 33](#) for information.

Deleting administrators

To delete an administrator or administrators, you must be logged in as a super user administrator.



You cannot delete an administrator that is currently logged in to the device.



The *admin* administrator can only be deleted using the CLI.

To delete an administrator or administrators:

1. Go to *System Settings > Admin > Administrators*.
2. Select the administrator or administrators you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the administrator or administrators.

To delete an administrator using the CLI:

1. Open a CLI console and enter the following command:

```
config system admin user
  delete <username>
end
```

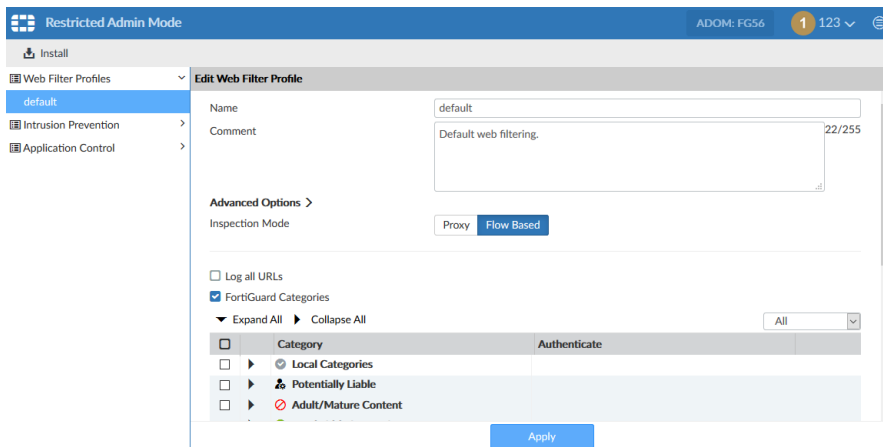
Restricted administrators

Restricted administrator accounts are used to delegate management of Web Filter, IPS, and Application Control profiles, and then install those objects to their assigned ADOM.



Restricted administrators cannot be used when workflow mode is enabled. See [Workflow Mode on page 65](#).

When a restricted administrators logs in to the FortiManager, they enter the *Restricted Admin Mode*. This mode consists of a simplified GUI where they can make changes to the profiles that they have access to, and then install those changes using the *Install* command in the toolbar, to their designated ADOM.

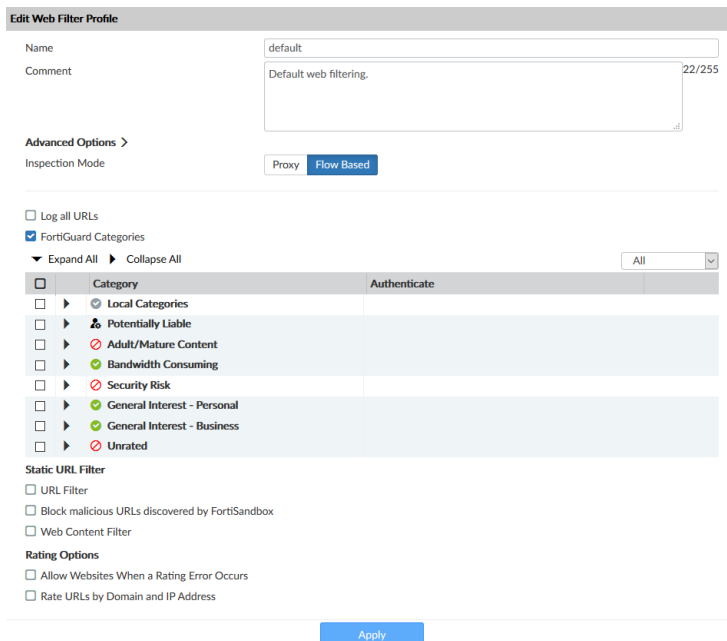


To create a restricted administrator:

1. Create an administrator profile with the *Type* set to *Restricted Admin* and the required permissions selected. See [Creating administrator profiles on page 89](#).
2. Create a new administrator and select the restricted administrator profile for the *Admin Profile*, then select the specific ADOM and profiles that the administrator can manage. See [Creating administrators on page 75](#)

Web Filter

Select a web filter profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.



Name	The profile name.
Comment	Optionally, enter a description of the profile.
Advanced Options	<p>Configure advanced options, including:</p> <ul style="list-style-type: none"> • <i>https-replacemsg</i>: enable/disable • <i>replacemsg-group</i>: select a group from the list • <i>web-filter-activex-log</i>: enable/disable • <i>web-filter-command-block-log</i>: enable/disable • <i>web-filter-cookie-removal-log</i>: enable/disable • <i>web-filter-js-log</i>: enable/disable • <i>web-filter-jscript-log</i>: enable/disable • <i>web-filter-referer-log</i>: enable/disable • <i>web-filter-unknown-log</i>: enable/disable • <i>web-filter-vbs-log</i>: enable/disable • <i>wisp</i>: enable/disable • <i>wisp-algorithm</i>: <i>auto-learning</i>, <i>primary-secondary</i>, or <i>round-robin</i>
Inspection Mode	Select <i>Proxy</i> or <i>Flow Based</i> .
Log all URLs	Select to log all URLs.
FortiGuard Categories	<p>Select FortiGuard categories.</p> <p>Right-click on a category to change the action: <i>Allow</i>, <i>Block</i>, <i>Warning</i>, <i>Monitor</i>, <i>Authenticate</i>, or, if available, <i>Disable</i>.</p> <p>Use the filter drop-down menu to filter the categories shown in the table based on the action.</p>
Allow Users to override blocked categories	<p>Select to allow users to override blocked categories.</p> <p>This option is only available if <i>Inspection Mode</i> is <i>Proxy</i>.</p>
Override Permit	Select the override permits: <i>bannedword-override</i> , <i>contenttype-check-override</i> , <i>fortiguard-wf-override</i> , and <i>urlfilter-override</i> .
Groups that can override	Select groups that can override blocked categories.
Profile can switch to	Select profiles that the user can switch to.
Switch applies to	Select what the switch applies to: <i>ask</i> , <i>browser</i> , <i>ip</i> , <i>user</i> , or <i>user-group</i> .
Switch Duration	Select the switch duration, either <i>ask</i> or <i>constant</i> .
Duration	<p>Enter the duration of the switch.</p> <p>This option is only available if <i>Switch Duration</i> is <i>constant</i>.</p>

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex	Select to enforce <i>Safe Search</i> . This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Restrict YouTube Access	Select to restrict access to YouTube. Select <i>Strict</i> or <i>Moderate</i> . This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Log all search keywords	Select to log all search keywords. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Block Invalid URLs	Select to block invalid URLs. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
URL Filter	Select to enable URL filters. Select URL filters from the dropdown list, and/or create and manage filters in the table.
Block malicious URLs discovered by FortiSandbox	Select to block URLs that FortiSandbox deems malicious.
Web Content Filter	Select to apply web content filters. Click <i>Add</i> to add filters to the table. Edit and delete filters as required.
Allow Websites When a Rating Error Occurs	Select to allow access to websites if a rating error occurs.
Rate URLs by Domain and IP Address	Select to rate URLs by both their domain and IP address.
Block HTTP Redirects by Rating	Select to block HTTP redirects based on the site's rating. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Rate Images by URL (Blocked images will be replaced with blanks)	Select to rate images based on the URL. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Restrict Google account usage to specific domains	Select to restrict Google account usage to specific domains. Click <i>Add</i> to add the domains to the table. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Provide Details for Blocked HTTP 4xx and 5xx Errors	Select to receive details about blocked HTTP errors. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
HTTP POST Action: Block	Select to set the HTTP POST action to block. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Remove Java Applet Filter	Select to remove the Java applet filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .
Remove ActiveX Filter	Select to remove the ActiveX filter. This option is only available if <i>Inspection Mode</i> is <i>Proxy</i> .

Remove Cookie Filter

Select to remove the cookie filter.

This option is only available if *Inspection Mode* is *Proxy*.

Intrusion Prevention

Select an IPS profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.

Edit IPS Profile

Name

all_default

Comments

All predefined signatures with default setting. 47/255

IPS Signatures

+ Add Signatures

✕ Delete

✎ Edit IP Exemptions

<input type="checkbox"/>	Name	Exempt IPs	Severity	Target	Service	OS	Action	Status	Packet Logging	Applications	ID	Revision
--------------------------	------	------------	----------	--------	---------	----	--------	--------	----------------	--------------	----	----------

IPS Filters

+ Add Filter

✎ Edit Filter

✕ Delete

<input type="checkbox"/>	Filter Details	Action	Packet Logging
<input type="checkbox"/>	Default	Default	✕

Rate Based Signatures

Enable	Signature	Threshold	Duration(Seconds)	Track By	Action	Block Duration
<input type="checkbox"/>	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	block	None
<input type="checkbox"/>	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	block	None
<input type="checkbox"/>	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	block	None
<input type="checkbox"/>	FTP.Login.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	FreeBSD.TCP.Reassembly.DoS	10	2	Any	block	None
<input type="checkbox"/>	IMAP.Login.Brute.Force	60	10	Any	block	None
<input type="checkbox"/>	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	block	None
<input type="checkbox"/>	MS.OWA.Brute.Force	15	1	Any	block	None
<input type="checkbox"/>	MS.RDP.Connection.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	MS.Windows.Group.Policy.Security.Feature.Bypass	5	2	Any	block	None
<input type="checkbox"/>	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	block	None
<input type="checkbox"/>	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	block	None
<input type="checkbox"/>	MS.XML.Core.Services.Memory.Corruption	5	10	Any	block	None
<input type="checkbox"/>	MySQL.Login.Brute.Force	60	60	Any	block	None
<input type="checkbox"/>	Novell.Open.Enterprise.Server.HTTPSTK.Service.DoS	18	1	Any	block	None
<input type="checkbox"/>	POP3.Login.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	SMB.Login.Brute.Force	500	60	Any	block	None
<input type="checkbox"/>	SSH.Connection.Brute.Force	200	10	Any	block	None
<input type="checkbox"/>	Telnet.Login.Brute.Force	60	60	Any	block	None
<input type="checkbox"/>	Wordpress.Login.Brute.Force	1000	10	Any	block	None

<

Advanced Options >

Apply

Name

The profile name.

Comment

Optionally, enter a description of the profile.

IPS Signatures

Click *Add Signatures* to add IPS signatures to the table. The signatures list can be filtered to simplify adding them.

To add or edit a signature's IP exemptions, select a signature then click *Edit IP Exemptions*.

Right-click on a signature to change the action (*Pass, Monitor, Block, Reset, Default, or Quarantine*), and to enable or disable *Packet Logging*.

IPS Filters

Click *Add Filter* to add IPS filters to the table. The filters list can be searched and filtered to simplify adding them.

Right-click on a signature to change the action (*Pass, Monitor, Block, Reset, Default, or Quarantine*), and to enable or disable *Packet Logging*.

Rate Based Signatures

Enable the required rate based signatures, then configure its options: *Threshold, Duration, Track By, Action, and Block Duration*.

Advanced Options

Enable or disable blocking malicious URLs.

Application Control

Select an application control profile from the tree menu to edit the profile details. Click *Apply* to apply any changes to the profile.

Edit Application Control Profile

Name: default

Comments: Monitor all applications. 25/255

Categories

<input type="checkbox"/> Monitor Botnet	<input type="checkbox"/> Monitor Game	<input type="checkbox"/> Monitor Proxy	<input type="checkbox"/> Monitor Video/Audio
<input type="checkbox"/> Monitor Business	<input type="checkbox"/> Monitor General.Interest	<input type="checkbox"/> Monitor Remote.Access	<input type="checkbox"/> Monitor VoIP
<input type="checkbox"/> Monitor Cloud.IT	<input type="checkbox"/> Monitor Mobile	<input type="checkbox"/> Monitor Social.Media	<input type="checkbox"/> Monitor Industrial
<input type="checkbox"/> Monitor Collaboration	<input type="checkbox"/> Monitor Network.Service	<input type="checkbox"/> Monitor Storage.Backup	<input type="checkbox"/> Monitor Web.Client
<input type="checkbox"/> Monitor Email	<input type="checkbox"/> Monitor P2P	<input type="checkbox"/> Monitor Update	<input checked="" type="checkbox"/> Allow Unknown Applications

Application Overrides

+ Add Signatures ☒ Edit Parameters ☐ Delete

Application Signature	Category	Action

Filter Overrides

+ Add Filter ☒ Edit ☐ Delete

Filter Details	Action

Options

☒ Deep Inspection of Cloud Applications

☒ Allow and Log DNS Traffic

☒ Replacement Messages for HTTP-based Applications

☐ Logging of Other Applications

☐ Logging of Unknown Applications

Advanced Options >

[Apply](#)

Name

The profile name.

Comment

Optionally, enter a description of the profile.

Categories

Select the action to take for each of the available categories: *Allow, Monitor, Block, Traffic Shaping, Quarantine, or Reset*.

Application Overrides	Click <i>Add Signatures</i> to add application override signatures to the table. The signatures list can be filtered to simplify adding them. Right-click on a signature to change the action (<i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Traffic Shaping</i> , <i>Quarantine</i> , or <i>Reset</i>).
Filter Overrides	Click <i>Add Filter</i> to add filter overrides to the table. The filters list can be searched and filtered to simplify adding them. Right-click on an override to change the action (<i>Allow</i> , <i>Monitor</i> , <i>Block</i> , <i>Traffic Shaping</i> , <i>Quarantine</i> , or <i>Reset</i>).
Deep Inspection of Cloud Applications	Select to enable deep inspections of cloud applications.
Allow and Log DNS Traffic	Select to allow and log DNS traffic.
Replacement Messages for HTTP-based Applications	Select to enable replacement messages for HTTP based applications.
Logging of Other Applications	Select to enable the logging of other applications.
Logging of Unknown Applications	Select to enable the logging of unknown applications.
Advanced Options	Configure advanced options: <ul style="list-style-type: none"> • p2p-black-list: Select from <i>bittorent</i>, <i>edonkey</i>, and <i>skype</i>. • replacemsg-group: Select an option from the dropdown list.

Administrator profiles

Administrator profiles are used to control administrator access privileges to devices or system features. Profiles are assigned to administrator accounts when an administrator is created. The profile controls access to both the FortiManager GUI and CLI.

There are four predefined system profiles:

Restricted_User	Restricted user profiles have no system privileges enabled, and have read-only access for all device privileges.
Standard_User	Standard user profiles have no system privileges enabled, and have read/write access for all device privileges.
Super_User	Super user profiles have all system and device privileges enabled. It cannot be edited.
Package_User	Package user profile have read/write policy and objects privileges enabled, and have read-only access for system and other privileges.

These profiles cannot be deleted, but standard and restricted profiles can be edited. New profiles can also be created as required. Only super user administrators can manage administrator profiles. Package user administrators can view the profile list.

Go to *System Settings > Admin > Profile* to view and manage administrator profiles.

+ Create New Edit Delete			
<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Restricted_User	System Admin	Restricted user profiles have no System Privileges enabled, and have read-only access for all Device Privileges.
<input type="checkbox"/>	Standard_User	System Admin	Standard user profiles have no System Privileges enabled, but have read/write access for all Device Privileges.
<input type="checkbox"/>	Super_User	System Admin	Super user profiles have all system and device privileges enabled.
<input type="checkbox"/>	Package_User	System Admin	Package user profile have read/write policy package and objects privileges enabled, and have read-only access for system and others privileges.
<input type="checkbox"/>	RatedR	Restricted Admin	

The following options are available:

Create New	Create a new administrator profile. See Creating administrator profiles on page 89 .
Edit	Edit the selected profile. See Editing administrator profiles on page 91 .
Delete	Delete the selected profile or profiles. See Deleting administrator profiles on page 91 .
Search	Search the administrator profiles list.

The following information is shown:

Name	The name the administrator uses to log in.
Type	The profile type, either <i>System Admin</i> or <i>Restricted Admin</i> .
Description	A description of the system and device access permissions allowed for the selected profile.

Permissions

The below table lists the default permissions for the predefined administrator profiles.

When *Read-Write* is selected, the user can view and make changes to the FortiManager system. When *Read-Only* is selected, the user can only view information. When *None* is selected, the user can neither view or make changes to the FortiManager system.

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
System Settings system-setting	Read-Write	None	None	Read-Only
Administrative Domain adom-switch	Read-Write	Read-Write	None	Read-Write

Setting		Predefined Administrator Profile			
		Super User	Standard User	Restricted User	Package User
FortiGuard Center fgd_center		Read-Write	None	None	Read-Only
	License Management fgd-center-licensing	Read-Write	None	None	Read-Only
	Firmware Management fgd-center-fmw-mgmt	Read-Write	None	None	Read-Only
	Advanced fgd-center-advanced	Read-Write	None	None	Read-Only
Device Manager device-manager		Read-Write	Read-Write	Read-Only	Read-Write
	Add/Delete Devices/Groups device-op	Read-Write	Read-Write	None	Read-Write
	Retrieve Configuration from Devices config-retrieve	Read-Write	Read-Write	Read-Only	Read-Only
	Revert Configuration from Revision History config-revert	Read-Write	Read-Write	Read-Only	Read-Only
	Terminal Access term-access	Read-Write	Read-Write	Read-Only	Read-Only
	Manage Device Configuration device-config	Read-Write	Read-Write	Read-Only	Read-Write
	Provisioning Templates device-profile	Read-Write	Read-Write	Read-Only	Read-Write
	SD-WAN device-wan-link-load-balance	Read-Write	Read-Write	Read-Only	Read-Write

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
Policy & Objects policy-objects	Read-Write	Read-Write	Read-Only	Read-Write
Global Policy Packages & Objects global-policy-packages	Read-Write	Read-Write	None	Read-Write
Assignment assignment	Read-Write	None	None	Read-Only
Policy Packages & Objects adom-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
Policy Check consistency-check	Read-Write	Read-Write	Read-Only	Read-Only
Install Policy Package or Device Configuration deploy-management	Read-Write	Read-Write	Read-Only	Read-Write
Import Policy Package import-policy-packages	Read-Write	Read-Write	Read-Only	Read-Write
Interface Mapping intf-mapping	Read-Write	Read-Write	Read-Only	Read-Write
AP Manager device-ap	Read-Write	Read-Write	Read-Only	Read-Write
FortiClient Manager device-forticlient	Read-Write	Read-Write	Read-Only	Read-Write
FortiSwitch Manager device-fortiswitch	Read-Write	Read-Write	Read-Only	Read-Write
VPN Manager vpn-manager	Read-Write	Read-Write	Read-Only	Read-Write
Log View/FortiView/NOC log-viewer	Read-Write	Read-Write	Read-Only	Read-Only
Event Management event-management	Read-Write	Read-Write	Read-Only	Read-Only
Reports report-viewer	Read-Write	Read-Write	Read-Only	Read-Only

Setting	Predefined Administrator Profile			
	Super User	Standard User	Restricted User	Package User
CLI only settings				
realtime-monitor	Read-Write	Read-Write	Read-Only	
read-passwd	Read-Write	None	None	Read-Only



The *Log View/FortiView/NOC*, *Event Management*, and *Reports* settings are only available when FortiAnalyzer features are enabled. See [FortiAnalyzer Features on page 390](#).

Creating administrator profiles

To create a new administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To create a custom administrator profile:

1. Go to *System Settings > Admin > Profile*.
2. Click *Create New* in the toolbar. The *New Profile* pane is displayed.

New Profile

Profile Name

Description

0/1023

Type

☒ System Admin
 ☐ Restricted Admin

Read-Write

Read-Only

None

System Settings	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Administrative Domain	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiGuard Center	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
License Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Firmware Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Advanced	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Device Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Add/Delete Devices/Groups	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Retrieve Configuration from Devices	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Revert Configuration from Revision History	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Terminal Access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Manage Device Configurations	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Provisioning Templates	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
SD-WAN	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Global Policy Packages & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Assignment	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Package & Objects	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Policy Check	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Install Policy Package or Device Configuration	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Import Policy Package	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Interface Mapping	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
AP Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiClient Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
FortiSwitch Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
VPN Manager	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Log View/FortiView/NOC	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Event Management	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Reports	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

OK

Cancel

3. Configure the following settings, and then click *OK* to create the new administrator profile.

Profile Name	Enter a name for this profile.
Description	Optionally, enter a description for this profile. While not a requirement, a description can help to know what the profiles is for, or the levels it is set to.
Type	Select the type of profile, either <i>System Admin</i> or <i>Restricted Admin</i> .
Permission	<p>Select which permissions to enable from <i>Web Filter Profile</i>, <i>Application Filter</i>, and <i>IPS Sensor</i>.</p> <p>This option is only available when <i>Type</i> is <i>Restricted Admin</i>. See Restricted administrators on page 79 for information.</p>
Permissions	<p>Select <i>None</i>, <i>Read Only</i>, or <i>Read-Write</i> access for the categories as required.</p> <p>This option is only available when <i>Type</i> is <i>System Admin</i>.</p>

Editing administrator profiles

To edit an administrator profile, you must be logged in to an account with sufficient privileges, or as a super user administrator. The profile's name cannot be edited. The *Super_User* profile cannot be edited, and the predefined profiles cannot be delete.

To edit an administrator:

1. Go to *System Settings > Admin > Profile*.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting administrator profiles

To delete a profile or profiles, you must be logged in to an account with sufficient privileges, or as a super user administrator. The predefined profiles cannot be deleted.

To delete a profile or profiles:

1. Go to *System Settings > Admin > Profile*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the profile or profiles.

Authentication

The FortiManager system supports authentication of administrators locally, remotely with RADIUS, LDAP, or TACACS+ servers, and using PKI. Remote authentication servers can also be added to authentication groups that administrators can use for authentication.

To use PKI authentication, you must configure the authentication before you create the administrator accounts. See [Public Key Infrastructure on page 91](#) for more information.

To use remote authentication servers, you must configure the appropriate server entries in the FortiManager unit for each authentication server in your network. New LDAP remote authentication servers can be added and linked to all ADOMs or specific ADOMs. See [LDAP servers on page 94](#), [RADIUS servers on page 96](#), and [TACACS+ servers on page 96](#) for more information.

Public Key Infrastructure

Public Key Infrastructure (PKI) authentication uses X.509 certificate authentication library that takes a list of peers, peer groups, and user groups and returns authentication successful or denied notifications. Administrators only need a valid X.509 certificate for successful authentication; no username or password is necessary.

To use PKI authentication for an administrator, you must configure the authentication before you create the administrator accounts. You will also need the following certificates:

- an X.509 certificate for the FortiManager administrator (administrator certificate)
- an X.509 certificate from the Certificate Authority (CA) which has signed the administrator's certificate (CA Certificate)

To get the CA certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > Certificate Authorities > Local CAs*.
3. Select the certificate and select *Export* in the toolbar to save the `ca_fortinet.com` CA certificate to your management computer. The saved CA certificate's filename is `ca_fortinet.com.crt`.

To get the administrator certificate:

1. Log into your FortiAuthenticator.
2. Go to *Certificate Management > End Entities > Users*.
3. Select the certificate and select *Export* in the toolbar to save the administrator certificate to your management computer. The saved CA certificate's filename is `admin_fortinet.com.p12`. This PKCS#12 file is password protected. You must enter a password on export.

To import the administrator certificate into your browser:

1. In Mozilla Firefox, go to *Options > Advanced > Certificates > View Certificates > Import*.
2. Select the file `admin_fortinet.com.p12` and enter the password used in the previous step.

To import the CA certificate into the FortiManager:

1. Log into your FortiManager.
2. Go to *System Settings > Certificates > CA Certificates*.
3. Click *Import*, and browse for the `ca_fortinet.com.crt` file you saved to your management computer, or drag and drop the file onto the dialog box. The certificate is displayed as `CA_Cert_1`.

To create a new PKI administrator account:

1. Go to *System Settings > Admin > Administrator*.
2. Click *Create New*. The *New Administrator* dialog box opens.
See [Creating administrators on page 75](#) for more information.
3. Select *PKI* for the *Admin Type*.
4. Enter a comment in the *Subject* field for the PKI administrator.
5. Select the CA certificate from the dropdown list in the *CA* field.
6. Click *OK* to create the new administrator account.



PKI authentication must be enabled via the FortiManager CLI with the following commands:

```
config system global
set clt-cert-reg enable
end
```



When connecting to the FortiManager GUI, you must use HTTPS when using PKI certificate authentication.



When both `set clt-cert-req` and `set admin-https-pki-required` are enabled, only PKI administrators can connect to the FortiManager GUI.

Managing remote authentication servers

The FortiManager system supports remote authentication of administrators using LDAP, RADIUS, and TACACS+ remote servers. To use this feature, you must configure the appropriate server entries for each authentication server in your network, see [LDAP servers on page 94](#), [RADIUS servers on page 96](#), and [TACACS+ servers on page 96](#) for more information.

Remote authentication servers can be added, edited, deleted, and added to authentication groups (CLI only).

Go to *System Settings > Admin > Remote Authentication Server* to manage remote authentication servers.

+ Create New ▾ Edit Delete				
<input type="checkbox"/>	▲ Name	Type	ADOM	Details
<input type="checkbox"/>	ActTack	TACACS+		10.10.10.15 CHAP
<input type="checkbox"/>	Dapple	LDAP	All ADOMs	10.10.10.11:389/cn:
<input type="checkbox"/>	Lapper	LDAP	Syslog, FortiAuthenticator, FortiCache, FortiMail, FortiWeb	10.10.10.55:389/cn:
<input type="checkbox"/>	Rader	RADIUS		10.10.10.13 PAP
<input type="checkbox"/>	Radium	RADIUS		10.11.10.10 10.11.11.10 MSv2

The following options are available:

Create New	Add an LDAP, RADIUS, or TACACS+ remote authentication server. See LDAP servers on page 94 , RADIUS servers on page 96 , and TACACS+ servers on page 96 .
Edit	Edit the selected remote authentication server. See Editing remote authentication servers on page 94 .
Delete	Delete the selected remote authentication server or servers. See Deleting remote authentication servers on page 94 .

The following information is displayed:

Name	The name of the server.
Type	The server type: <i>LDAP</i> , <i>RADIUS</i> , or <i>TACACS+</i> .
ADOM	The administrative domain(s) which are linked to the remote authentication server.
Details	Details about the server, such as the IP address.

Editing remote authentication servers

To edit a remote authentication server, you must be logged in to an account with sufficient privileges, or as a super user administrator. The server's name cannot be edited.

To edit a remote authentication server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select the server then click *Edit* in the toolbar. The *Edit Server* pane for that server type opens.
3. Edit the settings as required, and then select *OK* to apply the changes.
See [LDAP servers on page 94](#), [RADIUS servers on page 96](#), and [TACACS+ servers on page 96](#) for more information.

Deleting remote authentication servers

To delete a remote authentication server or servers, you must be logged in to an account with sufficient privileges, or as a super user administrator.

To delete a remote authentication server or servers:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the server or servers.

LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

If you have configured LDAP support and an administrator is required to authenticate using an LDAP server, the FortiManager unit sends the administrator's credentials to the LDAP server for authentication. If the LDAP server can authenticate the administrator, they are successfully authenticated with the FortiManager unit. If the LDAP server cannot authenticate the administrator, the FortiManager unit refuses the connection.

To use an LDAP server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add an LDAP server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select *Create New > LDAP Server* from the toolbar. The *New LDAP Server* pane opens.

The screenshot shows the 'New LDAP Server' configuration window. It has a title bar 'New LDAP Server'. Below it are several input fields and dropdown menus: 'Name' (text box), 'Server Name/IP' (text box), 'Port' (text box with '389' and a refresh icon), 'Common Name Identifier' (text box with 'cn'), 'Distinguished Name' (text box with a query icon), 'Bind Type' (dropdown menu with 'Simple' selected), 'Secure Connection' (checkbox checked), 'Protocol' (dropdown menu), 'Certificate' (dropdown menu with 'No Certificate' selected), and 'Administrative Domain' (button 'All ADOMs' and 'Specify'). At the bottom are 'OK' and 'Cancel' buttons.

3. Configure the following settings, and then click *OK* to add the LDAP server.

Name	Enter a name to identify the LDAP server.
Server Name/IP	Enter the IP address or fully qualified domain name of the LDAP server.
Port	Enter the port for LDAP traffic. The default port is 389.
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use <i>cn</i> . However, some servers use other common name identifiers such as <i>UID</i> .
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier. Clicking the <i>query distinguished name</i> icon will query the LDAP server for the name and open the <i>LDAP Distinguished Name Query</i> window to display the results.
Bind Type	Select the type of binding for LDAP authentication: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> .
User DN	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the user DN.
Password	When the <i>Bind Type</i> is set to <i>Regular</i> , enter the password.
Secure Connection	Select to use a secure LDAP server connection for authentication.
Protocol	When <i>Secure Connection</i> is enabled, select either LDAPS or STARTTLS.
Certificate	When <i>Secure Connection</i> is enabled, select the certificate from the dropdown list.
Administrative Domain	Choose the ADOMs this server will be linked to: <i>All ADOMs</i> , or <i>Specify</i> for specific ADOMs.

RADIUS servers

Remote Authentication Dial-in User (RADIUS) is a user authentication and network-usage accounting system. When users connect to a server they type a user name and password. This information is passed to a RADIUS server, which authenticates the user and authorizes access to the network.

You can create or edit RADIUS server entries in the server list to support authentication of administrators. When an administrator account's type is set to RADIUS, the FortiManager unit uses the RADIUS server to verify the administrator password at log on. The password is not stored on the FortiManager unit.

To use a RADIUS server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a RADIUS server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select *Create New > RADIUS Server* from the toolbar. The *New RADIUS Server* pane opens.

The screenshot shows a 'New RADIUS Server' configuration window. It has the following fields: 'Name' (text input), 'Server Name/IP' (text input), 'Port' (spin box with 1812), 'Server Secret' (text input), 'Secondary Server Name/IP' (text input), 'Secondary Server Secret' (text input), and 'Authentication Type' (dropdown menu). At the bottom right are 'OK' and 'Cancel' buttons.

3. Configure the following settings, and then click *OK* to add the RADIUS server.

Name	Enter a name to identify the RADIUS server.
Server Name/IP	Enter the IP address or fully qualified domain name of the RADIUS server.
Port	Enter the port for RADIUS traffic. The default port is 1812. Some RADIUS servers use port 1645.
Server Secret	Enter the RADIUS server secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary RADIUS server.
Secondary Server Secret	Enter the secondary RADIUS server secret.
Authentication Type	Select the authentication type the RADIUS server requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types.

TACACS+ servers

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other network computing devices via one or more centralized servers. It allows a client to accept a user name and password and send a query to a TACACS authentication server. The server

host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user. The default TCP port for a TACACS+ server is 49.

If you have configured TACACS+ support and an administrator is required to authenticate using a TACACS+ server, the FortiManager unit contacts the TACACS+ server for authentication. If the TACACS+ server can authenticate the administrator, they are successfully authenticated with the FortiManager unit. If the TACACS+ server cannot authenticate the administrator, the connection is refused by the FortiManager unit.

To use a TACACS+ server to authenticate administrators, you must configure the server before configuring the administrator accounts that will use it.

To add a TACACS+ server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Select *Create New > TACACS+ Server* from the toolbar. The *New TACACS+ Server* pane opens.

3. Configure the following settings, and then click *OK* to add the TACACS+ server.

Name	Enter a name to identify the TACACS+ server.
Server Name/IP	Enter the IP address or fully qualified domain name of the TACACS+ server.
Port	Enter the port for TACACS+ traffic. The default port is 49.
Server Key	Enter the key to access the TACACS+ server. The server key can be a maximum of 16 characters in length.
Authentication Type	Select the authentication type the TACACS+ server requires. If you select the default <i>ANY</i> , FortiManager tries all authentication types.

Remote authentication server groups

Remote authentication server groups can be used to extend wildcard administrator access. Normally, a wildcard administrator can only be created for a single server. If multiple servers of different types are grouped, a wildcard administrator can be applied to all of the servers in the group.

Multiple servers of the same type can be grouped to act as backups - if one server fails, the administrator can still be authenticated by another server in the group.

To use a server group to authenticate administrators, you must configure the group before configuring the administrator accounts that will use it.

Remote authentication server groups can only be managed using the CLI. For more information, see the [FortiManager CLI Reference](#).

To create a new remote authentication server group:

1. Open the admin group command shell:
`config system admin group`
2. Create a new group, or edit an already create group:
`edit <group name>`
3. Add remote authentication servers to the group:
`set member <server name> <server name> ...`
4. Apply your changes:
`end`

To edit the servers in a group:

1. Enter the following CLI commands:
`config system admin group`
`edit <group name>`
`set member <server name> <server name> ...`
`end`

Only the servers listed in the command will be in the group.

To remove all the servers from the group:

1. Enter the following CLI commands:
`config system admin group`
`edit <group name>`
`unset member`
`end`

All of the servers in the group will be removed.

To delete a group:

1. Enter the following CLI commands:
`config system admin group`
`delete <group name>`
`end`

Global administration settings

The administration settings page provides options for configuring global settings for administrator access to the FortiManager device. Settings include:

- Ports for HTTPS and HTTP administrative access

To improve security, you can change the default port configurations for administrative connections to the FortiManager. When connecting to the FortiManager unit when the port has changed, the port must be included, such as `https://<ip_address>:<port>`. For example, if you are connecting to the FortiManager unit using port 8080, the URL would be `https://192.168.1.99:8080`. When you change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is unique.

- Idle timeout settings

By default, the GUI disconnects administrative sessions if no activity occurs for five minutes. This prevents someone from using the GUI if the management computer is left unattended.

- GUI language

The language the GUI uses. For best results, you should select the language used by the management computer.

- GUI theme

The default color theme of the GUI is *Blueberry*. You can choose another color or an image.

- Password policy

Enforce password policies for administrators.

- Display options

Display or hide advanced configuration options in the GUI. Only the *admin* administrator can configure these options.



Only super user administrators can access and configure the administration settings. The settings are global and apply to all administrators of the FortiManager unit.

To configure the administration settings:

1. Go to *System Settings > Admin > Admin Settings*.

Admin Settings

Administration Settings

HTTP Port: 80

HTTPS Port: 443

HTTPS & Web Service Certificate: server.crt

Idle Timeout: 478 (1-480 Minutes)

☒ Redirects to HTTPS

View Settings

Language: Auto Detect

Theme: Blueberry (selected), Kiwi, Cherry, Plum, Spring, Summer, Autumn, Winter, 3D Structure, Aquarium, Binary Tunnel, Diving, Dreamy, Technology, Honey Bee, Twilight, Mountain, Northern Light, Astronomy, Fish, Penguin, Panda, Polar Bear, Parrot, Linked World

Password Policy

Minimum Length: 8 (8-32 characters)

Must Contain: ☐ Uppercase Letters, ☐ Lowercase Letters, ☐ Numbers (0-9), ☐ Special Characters

Admin Password Expires after: 0 (days)

Display Options on GUI

☒ Show Scripts, ☒ Show Add Multiple Button, ☒ Show Device List Import/Export Buttons

Apply

2. Configure the following settings as needed, then click *Apply* to save your changes to all administrator accounts:

Administration Settings

HTTP Port

Enter the TCP port to be used for administrative HTTP access. Default: 80.
Select *Redirect to HTTPS* to redirect HTTP traffic to HTTPS.

HTTPS Port

Enter the TCP port to be used for administrative HTTPS access. Default: 443.

HTTPS & Web Service Server Certificate	Select a certificate from the dropdown list.
Idle Timeout	Enter the number of minutes an administrative connection can be idle before the administrator must log in again, from 1 to 480 (8 hours). See Idle timeout on page 102 for more information.
View Settings	
Language	Select a language from the dropdown list. See GUI language on page 101 for more information.
Theme	Select a theme for the GUI. The selected theme is not applied until you click <i>Apply</i> , allowing to you to sample different themes. Default: Blueberry.
Password Policy	Click to enable administrator password policies. See Password policy on page 100 and Password lockout and retry attempts on page 101 for more information.
Minimum Length	Select the minimum length for a password, from 8 to 32 characters. Default: 8.
Must Contain	Select the types of characters a password must contain.
Admin Password Expires after	Select the number of days a password is valid for, after which it must be changed.
Display Options on GUI	Click to expand the display options.
Show Script	Display the <i>Script</i> menu item. This menu is located on the <i>Device Manager</i> pane. This is an advanced FortiManager feature.
Show Add Multiple Button	Display the <i>Add Multiple Devices</i> option. This option is located on the <i>Device Manager > Devices & Groups</i> pane, under the <i>More</i> option in the toolbar. This is an advanced FortiManager feature.
Show Device List Import/Export	Select to display the <i>Import Device List</i> and <i>Export Device List</i> buttons. This option is located on the <i>Device Manager > Devices & Groups</i> pane, under the <i>More</i> option in the toolbar. This is an advanced FortiManager feature.

Password policy

You can enable and configure password policy for the FortiManager.

To configure the password policy:

1. Go to *System Settings > Admin > Admin Settings*.
2. Click to enable *Password Policy*.
3. Configure the following settings, then click *Apply* to apply to password policy.

Minimum Length	Specify the minimum number of characters that a password must be, from 8 to 32. Default: 8.
Must Contain	Specify the types of characters a password must contain: uppercase and lowercase letters, numbers, and/or special characters.
Admin Password Expires after	Specify the number of days a password is valid for. When the time expires, an administrator will be prompted to enter a new password.

Password lockout and retry attempts

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be customized. Both settings can be configured using the CLI.

To configure the lockout duration:

1. Enter the following CLI commands:

```
config system global
    set admin-lockout-duration <seconds>
end
```

To configure the number of retry attempts:

1. Enter the following CLI commands:

```
config system global
    set admin-lockout-threshold <failed_attempts>
end
```

Example

To set the lockout threshold to one attempt and set a five minute duration before the administrator can try to log in again, enter the following CLI commands:

```
config system global
    set admin-lockout-duration 300
    set admin-lockout-threshold 1
end
```

GUI language

The GUI supports multiple languages, including:

- English
- Simplified Chinese
- Traditional Chinese
- Japanese
- Korean

By default, the GUI language is set to *Auto Detect*, which automatically uses the language used by the management computer. If that language is not supported, the GUI defaults to English. For best results, you should select the language used by the operating system on the management computer.

For more information about language support, see the [FortiManager Release Notes](#).

To change the GUI language:

1. Go to *System Settings > Admin > Admin Settings*.
2. Under the *View Settings*, In the *Language* field, select a language, or *Auto Detect*, from the dropdown list.
3. Click *Apply* to apply the language change.

Idle timeout

To ensure security, the idle timeout period should be short. By default, administrative sessions are disconnected if no activity takes place for five minutes. This idle timeout is recommended to prevent anyone from using the GUI on a PC that was logged in to the GUI and then left unattended. The idle timeout period can be set from 1 to 480 minutes.

To change the idle timeout:

1. Go to *System Settings > Admin > Admin Settings*.
2. Change the *Idle Timeout* period as required.
3. Click *Apply*.

Two-factor authentication

To configure two-factor authentication for administrators you will need the following:

- FortiManager
- FortiAuthenticator
- FortiToken

Configuring FortiAuthenticator

On the FortiAuthenticator, you must create a local user and a RADIUS client.



Before proceeding, ensure you have configured your FortiAuthenticator, created a NAS entry for your FortiManager, and created or imported FortiTokens.

For more information, see the *Two-Factor Authenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* in the [Fortinet Document Library](#).

To create a local user:

1. Go to *Authentication > User Management > Local Users*.
2. Click *Create New* in the toolbar.

3. Configure the following settings:

Username	Enter a user name for the local user.
Password creation	Select Specify a password from the dropdown list.
Password	Enter a password. The password must be a minimum of 8 characters.
Password confirmation	Re-enter the password. The passwords must match.
Allow RADIUS authentication	Enable to allow RADIUS authentication.
Role	Select the role for the new user.
Enable account expiration	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .

4. Click **OK** to continue to the *Change local user* page.

5. Configure the following settings, then click **OK**.

Disabled	Select to disable the local user.
Password-based authentication	Leave this option selected. Select <i>[Change Password]</i> to change the password for this local user.
Token-based authentication	Select to enable token-based authentication.
Deliver token code by	Select to deliver token by FortiToken, email, or SMS. Click <i>Test Token</i> to test the token.
Allow RADIUS authentication	Select to allow RADIUS authentication.
Enable account expiration	Optionally, select to enable account expiration. For more information see the <i>FortiAuthenticator Administration Guide</i> .
User Role	
Role	Select either <i>Administrator</i> or <i>User</i> .

Full Permission	Select to allow Full Permission, otherwise select the admin profiles to apply to the user. This option is only available when <i>Role</i> is <i>Administrator</i> .
Web service	Select to allow Web service, which allows the administrator to access the web service via a REST API or by using a client application. This option is only available when <i>Role</i> is <i>Administrator</i> .
Restrict admin login from trusted management subnets only	Select to restrict admin login from trusted management subnets only, then enter the trusted subnets in the table. This option is only available when <i>Role</i> is <i>Administrator</i> .
Allow LDAP Browsing	Select to allow LDAP browsing. This option is only available when <i>Role</i> is <i>User</i> .

To create a RADIUS client:

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name for the RADIUS client entry.
Client name/IP	Enter the IP address or Fully Qualified Domain Name (FQDN) of the FortiManager.
Secret	Enter the server secret. This value must match the FortiManager RADIUS server setting at <i>System Settings > Admin > Remote Authentication Server</i> .
First profile name	See the <i>FortiAuthenticator Administration Guide</i> .
Description	Enter an optional description for the RADIUS client entry.
Apply this profile based on RADIUS attributes	Select to apply the profile based on RADIUS attributes.
Authentication method	Select <i>Enforce two-factor authentication</i> from the list of options.
Username input format	Select specific user name input formats.
Realms	Configure realms.
Allow MAC-based authentication	Optional configuration.
Check machine authentication	Select to check machine based authentication and apply groups based on the success or failure of the authentication.
Enable captive portal	Enable various portals.
EAP types	Optional configuration.



For more information, see the *FortiAuthenticator Administration Guide*, available in the [Fortinet Document Library](#).

Configuring FortiManager

On the FortiManager, you need to configure the RADIUS server and create an administrator that uses the RADIUS server for authentication.

To configure the RADIUS server:

1. Go to *System Settings > Admin > Remote Authentication Server*.
2. Click *Create New > RADIUS* in the toolbar.
3. Configure the following settings, then click *OK*.

Name	Enter a name to identify the FortiAuthenticator.
Server Name/IP	Enter the IP address or fully qualified domain name of your FortiAuthenticator.
Server Secret	Enter the FortiAuthenticator secret.
Secondary Server Name/IP	Enter the IP address or fully qualified domain name of the secondary FortiAuthenticator, if applicable.
Secondary Server Secret	Enter the secondary FortiAuthenticator secret, if applicable.
Port	Enter the port for FortiAuthenticator traffic.
Authentication Type	<p>Select the authentication type the FortiAuthenticator requires. If you select the default <i>ANY</i>, FortiManager tries all authentication types.</p> <p>Note: RADIUS server authentication for local administrator users stored in FortiAuthenticator requires the <i>PAP</i> authentication type.</p>

To create the administrator:

1. Go to *System Settings > Admin > Administrator*.
2. Click *Create New* from the toolbar.
3. Configure the settings, selecting the previously added RADIUS server from the *RADIUS Server* dropdown list. See [Creating administrators on page 75](#).
4. Click *OK* to save the settings.

To test the configuration:

1. Attempt to log in to the FortiManager GUI with your new credentials.
2. Enter your user name and password and click *Login*.
3. Enter your FortiToken pin code and click *Submit* to log in to the FortiManager.

Device Manager

Use the *Device Manager* pane to add, configure, and manage devices.

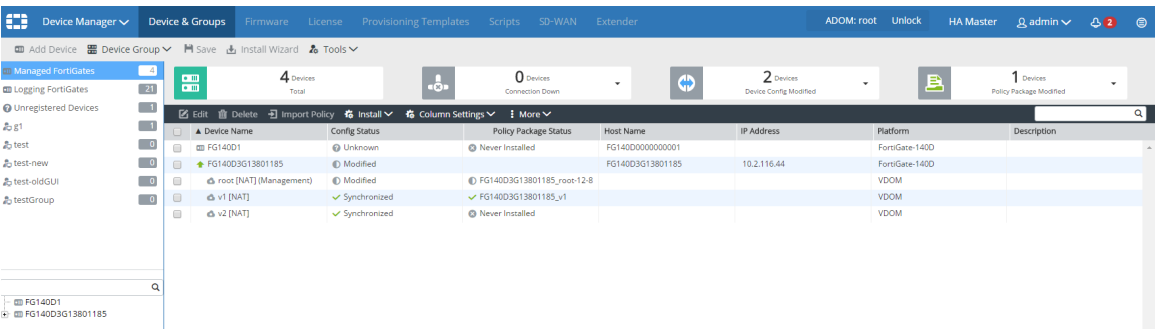
This topic covers navigating the *Device Manager* pane, adding devices, and managing devices. It also covers managing FortiExtender wireless WAN extenders.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click the mouse on different parts of the navigation panes on the GUI page to access these context menus.



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 64](#).



The *Device Manager* pane includes the following tabs in the blue banner:

Device & Groups	Add, configure, and view managed and logging devices. Use the toolbar to add devices, devices groups, and launch the install wizard. See Adding devices on page 107 . The <i>Device & Groups</i> tab also contains a quick status bar for a selected device group. See Using the quick status bar on page 138 .
Firmware	View information about firmware for devices as well as upgrade firmware. See Firmware on page 151 .
License	View license information for devices as well as push license updates to devices. See License on page 153 .
Provisioning Templates	Configure provisioning templates. For information on system, Threat Weight, FortiClient, and certificate templates, see Provisioning Templates on page 155 .
Scripts	Create new or import scripts. Scripts is disabled by default. You can enable this advanced configuration option in <i>System Systems > Admin > Admin Settings</i> . Select <i>Show Script</i> to enable on this option in the <i>Device Manager</i> pane. See Scripts on page 159 .

SD-WAN

Configure profiles for load balancing SD-WAN links and monitor load-balancing profiles. The *SD-WAN* tab is displayed only when central SD-WAN Link load balancing is enabled. See [SD-WAN Load Balance on page 192](#).

FortiExtender

View and configure FortiExtender. See [FortiExtender on page 195](#).

ADOMs

You can organize connected devices into ADOMs to better manage the devices. ADOMs can be organized by:

- Firmware version: group all 5.4 devices into one ADOM, and all 5.2 devices into another.
- Geographic regions: group all devices for a specific geographic region into an ADOM, and devices for a separate region into another ADOM.
- Administrator users: group devices into separate ADOMs based for specific administrators responsible for the group of devices.
- Customers: group all devices for one customer into an ADOM, and devices for another customer into another ADOM.

FortiAnalyzer, FortiCache, FortiClient, FortiDDos, FortiMail, FortiManager, FortiSandbox, FortiWeb, Chassis, and FortiCarrier devices are automatically placed in their own ADOMs.

Each administrator profile can be customized to provide read-only, read/write, or restrict access to various ADOM settings. When creating new administrator accounts, you can restrict which ADOMs the administrator can access, for enhanced control of your administrator users. For more information on ADOM configuration and settings, see [Administrative Domains on page 53](#).



For information on adding devices to an ADOM by using the *Add Device* wizard, see [Adding devices using the wizard on page 108](#).

Adding devices

You must add devices to the FortiManager system to use FortiManager to manage the devices. You must also enable *Central Management* on the managed device by using FortiOS. You can add an existing, operational device or an unregistered device. You can also provision a new device.

You can add individual devices or multiple devices. Adding devices using the *Add Device* wizard gives you more configuration options than using *Add Multiple* devices.

For a device that is currently online, use the *Add Device* wizard, select *Discover*, and follow the steps in the wizard. Adding an existing device does not result in an immediate connection to the device. Device connection happens only when you successfully synchronize the device. To provision a new device which is not yet online, use the *Add Device* wizard and select *Add Model Device*.

Adding an operating FortiGate HA cluster to the *Device Manager* pane is similar to adding a standalone device. Type the IP address of the master device, the FortiManager handles a cluster as a single managed device.

Adding devices using the wizard

You can add devices to the FortiManager unit by using the *Add Device* wizard. You can use the wizard to discover devices or add model devices to your FortiManager unit.



You cannot use the *Add Device* wizard to add FortiAnalyzer to FortiManager. You must use the *Add FortiAnalyzer* wizard instead. See [Adding FortiAnalyzer devices on page 119](#).

Use the *Discover* option for devices that are currently online and discoverable on your network.

Use the *Add Model Device* option to add a device that is not yet online. You can configure a model device to automatically register with FortiManager when the device is online.



When configuring a model device to automatically promote or register with FortiManager, add the model device to FortiManager by using a pre-shared key. When the device connects to FortiManager, run the `execute central-mgmt register-device` command from the FortiGate console. The device is automatically promoted or registered, and the configuration of the matched model device is applied.

For FortiOS 5.4.1 or earlier, you must run the `execute central-mgmt register-device` command.



To confirm that a device model or firmware version is supported by current firmware version running on FortiManager run the following CLI command:

```
diagnose dvm supported-platforms list
```

Adding a device using Discover mode

The following steps will guide you through the *Add Device* wizard phases to add a device using *Discover* mode.

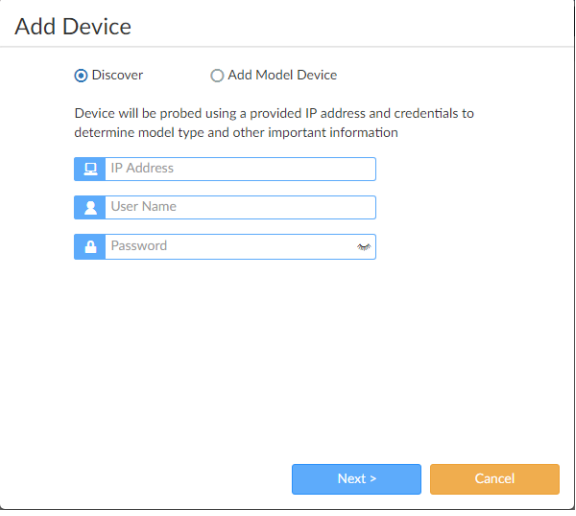


FortiManager will not be able to communicate with the FortiGate if offline mode is enabled. Enabling offline mode will prevent FortiManager from discovering devices.

To add a device using Discover mode:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.

3. Click **Add Device**. The wizard opens.



The 'Add Device' wizard is shown with the 'Discover' option selected. It contains three input fields: 'IP Address', 'User Name', and 'Password'. A 'Next >' button is at the bottom right.

Add Device

☒ Discover ☐ Add Model Device

Device will be probed using a provided IP address and credentials to determine model type and other important information

IP Address

User Name

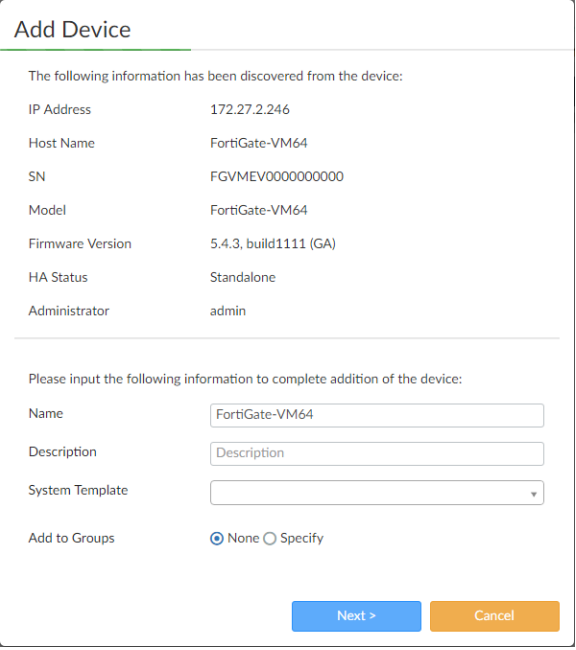
Password

Next > Cancel

4. Select **Discover**. Type the IP address, user name, and password for the device, then click **Next**.

FortiManager probes the IP address on your network to discover device details, including:

- IP address
- Host name
- Serial number
- Device model
- Firmware version and build
- High Availability status
- Administrator user name



The 'Add Device' wizard shows the discovered information from the device. It includes a table with fields like IP Address, Host Name, SN, Model, Firmware Version, HA Status, and Administrator. Below the table, there are input fields for Name, Description, and System Template, and a section for 'Add to Groups' with radio buttons for 'None' and 'Specify'.

Add Device

The following information has been discovered from the device:

IP Address	172.27.2.246
Host Name	FortiGate-VM64
SN	FGVMEV0000000000
Model	FortiGate-VM64
Firmware Version	5.4.3, build1111 (GA)
HA Status	Standalone
Administrator	admin

Please input the following information to complete addition of the device:

Name: FortiGate-VM64

Description: Description

System Template: [Dropdown]

Add to Groups: ☒ None ☐ Specify

Next > Cancel

5. Configure the following settings:

Name	Type a unique name for the device. The device name cannot contain spaces or special characters.
Description	Type a description of the device (optional).
System Template	System templates can be used to centrally manage certain device-level options from a central location. If required, assign a system template using the dropdown menu. Alternatively, you can select to configure all settings per-device inside <i>Device Manager</i> . For more information, see Provisioning Templates on page 155 .
Add to Groups	Select to add the device to any predefined groups.

6. Click *Next*.

The wizard discovers the device, and performs some or all of the following checks:

- Discovering device
- Creating device database
- Initializing configuration database
- Retrieving configuration
- Retrieving support data
- Updating group membership
- Successfully add device
- Check device status

Add Device

Name: FortiGate-VM64

IP Address: 172.27.2.246

Status: 50%

- ✓ Discovering device
- ✓ Creating device database
- ✓ Initializing configuration database
- Retrieving configuration
- Retrieving support data
- Updating group membership
- Successfully add device
- Check Device Status

Cancel

After the wizard completes the checks, you are asked to choose whether to import policies and objects for the device now or later.

7. Click *Import Later* to finish adding the device and close the wizard.

If you click *Import Now*, the wizard continues. The next step in the wizard depends on whether you are importing a FortiGate VDOM.

If you are importing a FortiGate VDOM, the following page is displayed with import options for the VDOM. Select an option, and click *Next*.

Import Device - FW148-1

Import Options

☒ Import each VDOM step by step

☐ Automatically import one VDOM at a time

☐ Automatically import all VDOMs

root
T4

Next > Cancel

If you are not importing a FortiGate VDOM, the following page is displayed.

Import Device - FortiGate-VM64 [root]

Create a new policy package for import.

Policy Package Name: FortiGate-VM64_root

Folder: root

Policy Selection

☒ Import All (1)

☐ Select Policies and Profile Groups to Import

Object Selection

☒ Import only policy dependent objects

☐ Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Searching for interface mappings on device ...

Next > Cancel

8. Set the following options, then click *Next*:
- In the *Policy Selection* section, select *Import All* or *Select Policies and Profile Groups to Import*.
 - In the *Object Selection* section, select *Import only policy dependent objects* or *Import all objects*.
 - Check the device interface mappings.
 - Select or clear the *Add mappings for all unused device interfaces* checkbox.
- The list of objects that will be updated is displayed.

Import Device - FortiGate-VM64 [root]

The following objects will be updated after import. Click 'Next' to start import process.

Duplicates (4) ▼

Address (1)	all	
Recurring Schedule (1)	always	
Service (1)	ALL	
Service Category (1)	General	

Next >
Cancel

9. Click *Next*.

A detailed summary of the import is shown. Click *Download Import Report* to download a report of the import. The report is only available on this page.

Import Device - FortiGate-VM64 [root]

✓ 1 policies and objects are imported. [\[Download Import Report\]](#)

Import Summary

Firewall Policy	1 of 1
-----------------	--------

Finish

10. Click *Finish* to finish adding the device and close the wizard.

Adding a model device

The following instructions will guide you through the *Add Device* wizard phases to add a device using *Add Model Device* mode.



To confirm that a device model or firmware version is supported by the FortiManager's current firmware version, run the following CLI command:

```
diagnose dvm supported-platforms list
```



When adding devices to product-specific ADOMs, you can only add that product type to the ADOM. When selecting to add a non-FortiGate device to the root ADOM, the device will automatically be added to the product specific ADOM.

To add a model device:

1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*. The *Add Device* wizard displays.

4. Click *Add Model Device* and enter the following information:

Add Model Device	Device will be added using the chosen model type and other explicitly entered information.
Name	Type a descriptive name for the device. This name is displayed in the <i>Device Name</i> column. Each device must have a unique name, otherwise the wizard will fail.
Link Device By	<p>The method by which the device will be added, either <i>Serial Number</i> or <i>Pre-Shared Key</i>.</p> <p>The serial number should be used if it is known. A pre-shared key can be used if the serial number is not known when the model device is added.</p> <p>If using a pre-shared key, the following CLI command needs to be issued from the FortiGate device when it is installed in the field:</p> <pre>execute central-mgmt register-device <fmg-serial-number> <preshared-key></pre>
Serial Number or Pre-Shared Key	<p>Type the device serial number or pre-shared key. This field is mandatory.</p> <p>If using a pre-shared key, each device must have a unique pre-shared key. You can change the pre-shared key after adding the model device. See Editing device information on page 139.</p>

Device Model	Select the device model from the list. If linking by serial number, the serial number must be entered before selecting a device model.
Firmware Version	Select the device's firmware version from the dropdown list.

5. Click *Next*. The device is created in the FortiManager database.

6. Click *Finish* to exit the wizard.

A device added using the *Add Model Device* option has similar dashboard options as a device added using the *Discover* option. As the device is not yet online, some options are not available.



A configuration file needs to be associated with the model device so that FortiManager will automatically install the configuration to the matching device when it connects to the FortiManager. FortiManager will not retrieve a configuration file from a real device that matches a model device.

Use the *Import Revision* function to associate a configuration file with the model device. See [Managing configuration revision history on page 147](#).

Example of adding a model device by pre-shared key

This section describes how to add a FortiGate model by using the pre-shared key for FortiGate. You must perform some steps using FortiManager and some steps using FortiOS.

To add a model device by pre-shared key:

1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*. The *Add Device* wizard displays.
4. Click *Add Model Device* and type a name for the model device.
5. In the *Link Device By* list, select *Pre-shared Key*, and type the pre-shared key from FortiGate.
6. Set the remaining options, and click *Next*. The device is created in the FortiManager database.
7. Click *Finish* to exit the wizard.

After the device model is added to FortiManager, you can use FortiManager to configure the model device.

8. In FortiOS, configure the FortiManager IP address or FQDN in device central management by using the following command:

```
config system central-management
  set type fortimanager
  set fmg {<ip address> | <FQDN>}
end
```

9. In FortiOS, use the following command to link the model device to the real device, and to install configurations to the real device:

```
exe central-mgmt register-device <fmg-serial-number> <pre-shared key>
```

After the command is executed, FortiManager automatically links the model device to the real device, and installs configurations to the device.

Example of adding a model device by serial number

This section describes how to add a FortiGate model device to FortiManager by using the serial number for the FortiGate. You must perform some steps using FortiManager and some steps using FortiOS.

To add a model device by serial number:

1. If ADOMs are enabled, select the ADOM to which you want to add the device.
2. Go to *Device Manager > Device & Groups*.
3. Click *Add Device*. The *Add Device* wizard displays.
4. Click *Add Model Device* and type a name for the model device.
5. In the *Link Device By* list, select *Serial Number* and type the serial number for the FortiGate unit.
6. Set the remaining options, and click *Next*. The device is created in the FortiManager database.
7. Click *Finish* to exit the wizard.
After the device model is added to FortiManager, you can use FortiManager to configure the model device.
8. In FortiOS GUI, configure the FortiManager IP address in device central management.
 - a. Go to *System > Settings*.
 - b. In the *Central Management* area, type the FortiManager IP address in the *IP/Domain Name* box, and click *Apply*.

FortiManager automatically links the model device to the real device, and installs configurations to the device.

Adding devices manually

You can manually add devices to the FortiManager unit. The process requires the following steps:

- In FortiOS, you must enable central management on the device by adding the IP address of the FortiManager unit. As a result, the device is displayed on the FortiManager GUI in the root ADOM on the *Device Manager* pane in the *Unregistered Devices* list.
- In FortiManager, you must manually add unregistered devices. As a result, the device is registered with the FortiManager unit, and you can use FortiManager to manage the device.

When ADOMs are enabled, the device must be assigned to an ADOM when it is registered.

To manually add devices:

1. In FortiOS, enable central management for the device.
2. In FortiManager, select the root ADOM, and go to *Device Manager*.
3. In the tree menu, click *Unregistered Devices*. The content pane displays the unregistered devices.
4. Select the unregistered device or devices, then click *Add*. The *Add Device* dialog box opens.

Device Name	Credential	Assign New Device Name
FGVM000000000	admin	FortiGate-VM64

5. If ADOMs are enabled, select the ADOM in the *Add the following device(s) to ADOM* list. If ADOMs are disabled, select *root*.
 6. Type the login and password for the device or devices.
 7. Click *OK* to register the device or devices.
- The device or devices are added.

Add a VDOM to a device

To add a VDOM to a managed FortiGate device, right-click on the content pane for a particular device and select *Add VDOM* from the pop-up menu.



The number of VDOMs you can add is dependent on the device model. For more information, see the *Maximum Values Table* in the [Fortinet Document Library](#).

To add a VDOM to a FortiGate device:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, click the group. The devices in the group are displayed in the content pane.
3. In the content pane, right-click a device, and select *Add VDOM*.

Add VDOM

Name

Description 0/255

Enable ☒

Operation Mode

Inspection Mode ☒ Proxy(Default) ☐ Flow-based

Interface Members

4. Configure the following options, and click *OK*.

Name	Type a name for the new virtual domain.
Description	Optionally, enter a description of the VDOM.
Enable	Select to enable the VDOM.
Operation Mode	Select either <i>NAT</i> or <i>Transparent</i> .
Inspection Mode	Select an inspection mode.
Interface Members	Click to select each port one by one.

Adding a security fabric group

Before you can add a security fabric group to FortiManager, you must create the security fabric group in FortiOS. For more information, see the *FortiOS Handbook*.

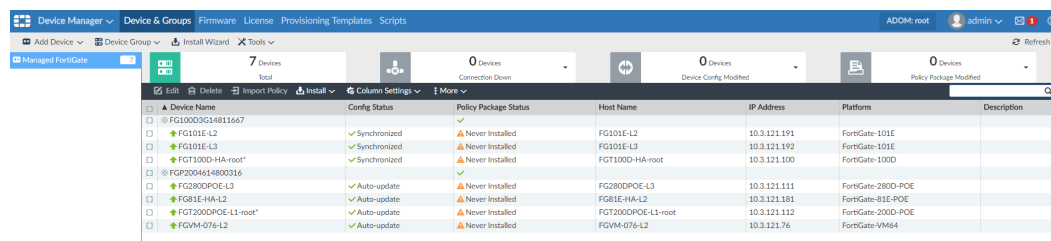
You must add to FortiManager the root FortiGate for the security fabric group as well as all FortiGate members of the security fabric group. Although you can add the root and member FortiGate units in any order to FortiManager, the added units are only recognized as part of a security fabric group after you add the root FortiGate.

See also [Displaying security fabric topology on page 143](#).

To add a security fabric group:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. Add the root FortiGate unit for the security fabric group. See [Adding a device using Discover mode on page 108](#).
4. Add each FortiGate unit that is a member of the security fabric group. See [Adding a device using Discover mode on page 108](#).
5. In the *Device Manager* content pane, right-click the root FortiGate unit, and select *Refresh*.

FortiManager retrieves information about the security fabric group via the root FortiGate unit. All units are displayed in a security fabric group. The *Security Fabric* icon identifies the group, and the group name is the serial number for the root FortiGate in the group. Within the group, a * at the end of the device name identifies the root FortiGate in the group.



Device Name	Config Status	Policy Package Status	Host Name	IP Address	Platform	Description
FG100D3G14B11667	✓ Synchronized	✓				
FG101E-L2	✓ Synchronized	⚠ Never Installed	FG101E-L2	10.3.121.191	FortGate-101E	
FG101E-L3	✓ Synchronized	⚠ Never Installed	FG101E-L3	10.3.121.192	FortGate-101E	
FGT100D-HA-root*	✓ Synchronized	⚠ Never Installed	FGT100D-HA-root	10.3.121.100	FortGate-100D	
FGP200A614800316	✓	✓				
FG280DPOE-L3	✓ Auto-update	⚠ Never Installed	FG280DPOE-L3	10.3.121.111	FortGate-280D-POE	
FG81E-HA-L2	✓ Auto-update	⚠ Never Installed	FG81E-HA-L2	10.3.121.181	FortGate-81E-POE	
FGT200DPOE-L1-root*	✓ Auto-update	⚠ Never Installed	FGT200DPOE-L1-root	10.3.121.112	FortGate-200D-POE	
FGVM-076-L2	✓ Auto-update	⚠ Never Installed	FGVM-076-L2	10.3.121.76	FortGate-VM64	

Import policy wizard

On the *Device Manager > Device & Groups* pane, right-click a device, and select *Import Policy* to launch the *Import Device* wizard. This wizard allows you to import interface maps, policy databases, and objects.



After initially importing policies from the device, make all changes related to policies and objects in *Policy & Objects* on the FortiManager.

Making changes directly on the FortiGate device will require reimporting policies to resynchronize the policies and objects.

Device Interface

The Device Interface page allows you to choose an ADOM interface for each device interface. When importing configuration from a device, all enabled interfaces require a mapping.

Interface maps will be created automatically for unmapped interfaces.

Import Device - FortiGate [root]

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	ADOM Interface
port1	port1
port2	port2
port3	port3
port4	port4
port5	port5
port6	port6
port7	port7
port8	port8
port9	port9

☒ Add mappings for all unused device interfaces

Next > Cancel

Select *Add mapping for all unused device interfaces* to automatically create interface maps for unused interfaces.

Policy

The policy page allows you to create a new policy package for import.

Select a folder from the dropdown menu, specify a policy package name, then configure the following options:

Policy Package Name	Type a name for the policy package.
Folder	Select a folder on the dropdown menu.
Policy Selection	Select to import all, or select specific policies and policies groups to import.
Object Selection	<p>Select <i>Import only policy dependent objects</i> to import policy dependent objects only for the device.</p> <p>Select <i>Import all objects</i> to import all objects for the selected device.</p>

Object

The object page will search for dependencies, and reports any conflicts it detects. If conflicts are detected, you must decide whether to use the FortiGate value or the FortiManager value. If there are conflicts, you can select *View Details* to view details of each individual conflict, or you can download an HTML conflict file to view all the details about the conflicts. Duplicates will not be imported.

Click *Next* to view the objects that are ready to be imported, and then click *Next* again to proceed with importing.

Import

Objects are imported into the common database, and the policies are imported into the selected package. Click *Next* to continue to the summary.



The import process removes all policies that have FortiManager generated policy IDs, such as 1073741825, that were previously learned by the FortiManager device. The FortiGate unit may inherit a policy ID from the global header policy, global footer policy, or VPN console.

Summary

The summary page allows you to download the import device summary results. It cannot be downloaded from anywhere else.

Adding FortiAnalyzer devices

Adding a FortiAnalyzer device to FortiManager gives FortiManager visibility into the logs on the FortiAnalyzer, providing a Single Pane of Glass on the FortiManager. It also enables FortiAnalyzer features, such as *NOC*, and *Log View*.

For information about FortiAnalyzer features, see [FortiAnalyzer Features on page 390](#). See also [Viewing policy rules on page 391](#) and [View logs related to a policy rule on page 227](#).



To add a FortiAnalyzer to FortiManager, they both must be running the same OS version, at least 5.6 or later.



If FortiAnalyzer features are enabled, you cannot add a FortiAnalyzer unit to the FortiManager. See [FortiAnalyzer Features on page 390](#).

In addition, you cannot add a FortiAnalyzer unit to the FortiManager when ADOMs are enabled and ADOM mode is set to *Advanced*.

ADOMs disabled

When you add a FortiAnalyzer device to FortiManager with ADOMs disabled, all devices with logging enabled can send logs to the FortiAnalyzer device. You can add only one FortiAnalyzer device to FortiManager, and the FortiAnalyzer device limit must be equal to or greater than the number of devices managed by FortiManager.

When you add additional devices with logging enabled to FortiManager, the managed devices can send logs to the FortiAnalyzer device. The new devices display in the *Device Manager* pane on FortiAnalyzer unit when FortiManager synchronizes with the FortiAnalyzer unit.

ADOMs enabled

When you add a FortiAnalyzer device to FortiManager with ADOMs enabled, all devices with logging enabled in the ADOM can send logs to the FortiAnalyzer device. Following are the guidelines for adding a FortiAnalyzer device to FortiManager when ADOMs are enabled:

- You can add one FortiAnalyzer device to each ADOM, and the FortiAnalyzer device limit must be equal to or greater than the number of devices in the ADOM.
- The same ADOM name and settings must exist on the FortiAnalyzer device and FortiManager. The wizard synchronizes these settings for you if there is a mismatch.
- The logging devices in the FortiAnalyzer ADOM and FortiManager ADOM must be the same. The wizard synchronizes these settings for you.
- You cannot add the same FortiAnalyzer device to multiple ADOMs.

When you add additional devices with logging enabled to an ADOM in FortiManager, the managed devices can send logs to the FortiAnalyzer device in the ADOM. The new devices display in the *Device Manager* pane on the FortiAnalyzer unit when FortiManager synchronizes with the FortiAnalyzer unit.

Provisioning templates for log settings

After you add a FortiAnalyzer device to FortiManager, you can use FortiManager to enable logging for all FortiGates in the root ADOM (when ADOMs are disabled) or the ADOM (when ADOMs are enabled) by using the log settings in a system template. See [System templates on page 155](#).

Legacy FortiAnalyzer ADOM

The FortiAnalyzer ADOM supports FortiAnalyzer units added to FortiManager before upgrading to FortiManager 5.6 and later. If you want to use the new functionality, you must delete the FortiAnalyzer unit from FortiManager and add it by using the Add FortiAnalyzer wizard.

Log storage and configuration

Logs are stored on the FortiAnalyzer device, not the FortiManager device. You configure log storage settings on the FortiAnalyzer device; you cannot change log storage settings using FortiManager.

Configuration and data for FortiAnalyzer features

When FortiManager manages a FortiAnalyzer unit, all configuration and data is kept on the FortiAnalyzer unit to support the following FortiAnalyzer features: *FortiView*, *Log View*, *Event Management*, and *Reports*. FortiManager remotely accesses the FortiAnalyzer unit to retrieve requested information for FortiAnalyzer features. For example, if you use the *Reports* pane in FortiManager to create a report, the report is created on the FortiAnalyzer unit and remotely accessed by FortiManager.

Adding FortiAnalyzer devices with the wizard

If the FortiAnalyzer unit is receiving logs from devices that are not managed by FortiManager, the wizard requires you to add the devices to FortiManager by typing the IP address and login credentials for each device. Ensure that you have the IP addresses and login credentials for each device before you start the wizard.



The *Add FortiAnalyzer* option is hidden when you cannot add a FortiAnalyzer unit to the FortiManager unit. For example, the *Add FortiAnalyzer* option is hidden if you have already added a FortiAnalyzer unit to the FortiManager unit (when ADOMs are disabled) or to the ADOM (when ADOMs are enabled). You also cannot add a FortiAnalyzer unit when you have enabled FortiAnalyzer features for the FortiManager unit.

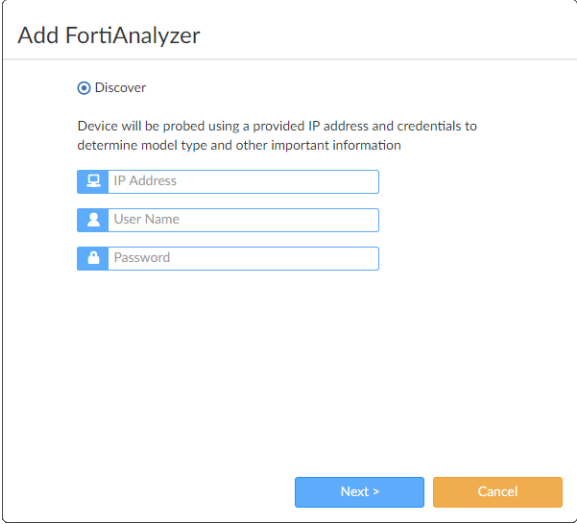


FortiManager and FortiAnalyzer must be running 5.6 or later, and the versions must be the same on both devices.

To add a FortiAnalyzer device:

1. Confirm that the FortiAnalyzer device supports the number of devices managed by FortiManager.
 - If ADOMs are disabled, ensure that the FortiAnalyzer device limit is equal to or greater than the number of devices managed by FortiManager.
 - If ADOMs are enabled, ensure that the FortiAnalyzer device limit is equal to or greater than the number of devices in the ADOM.
2. If ADOMs are enabled, select the ADOM to which you want to add the device.
3. Go to *Device Manager > Device & Groups*.
4. Click *Add Device > Add FortiAnalyzer*. The wizard opens.

The *Add FortiAnalyzer* option is hidden if you've already added a FortiAnalyzer device.



5. Type the IP address, user name, and password for the device, then click *Next*.
FortiManager probes the IP address on your network to discover FortiAnalyzer device details, including:
 - IP address
 - Host name
 - Serial number
 - Device model
 - Firmware version (build)
 - High Availability status
 - Administrator user name

Add FortiAnalyzer

The following information has been discovered from the device:

IP Address	172.27.2.223
Host Name	FAZVM64
SN	FAZ-VM0000000001
Model	FortiAnalyzer-VM64
Firmware Version	5.6.0, build1530 (GA)
HA Status	Standalone
Administrator	admin

Please input the following information to complete addition of the device:

Name	<input type="text" value="FAZVM64"/>
Description	<input type="text" value="Description"/>

[Next >](#)
[Cancel](#)

6. Configure the following settings if desired, and click *Next*:

Name Type a unique name for the device. The device name cannot contain spaces or special characters (optional).

Description Type a description of the device (optional).

The wizard performs the following tasks:

- Compares the ADOM name and configuration as well as devices between FortiAnalyzer and FortiManager
- Verifies the devices in the *Device Manager* pane for FortiAnalyzer with the devices in the *Device Manager* pane for FortiManager

If any discrepancies are found, information is displayed in the *Status* column, and you can resolve the discrepancies by clicking the *Synchronize ADOM and Devices* button.

Add FortiAnalyzer

Status: Verifying managed/logging devices on both sides...

50%		
Status	Device Name	Platform
Sync	FGVM010000092070	FortiGate-VM64

[Synchronize ADOM and Devices](#)
[Cancel](#)

The following table describes the different statuses:

Status	Description
FMG Only	The device was located in FortiManager, but not FortiAnalyzer. If you proceed with the wizard, the device will be added to FortiAnalyzer too.
FAZ Only	The device was located in FortiAnalyzer, but not FortiManager. If you proceed with the wizard, the device will be added to FortiManager too. The login and password for the device is required to complete the wizard.
Sync	The device was located in both FortiAnalyzer and FortiManager without any differences, and the wizard will synchronize the device between FortiManager and FortiAnalyzer.

Status	Description
Mismatched	The device was located in both FortiAnalyzer and FortiManager with some differences, and the wizard will synchronize the device settings between FortiManager and FortiAnalyzer to remove the differences.

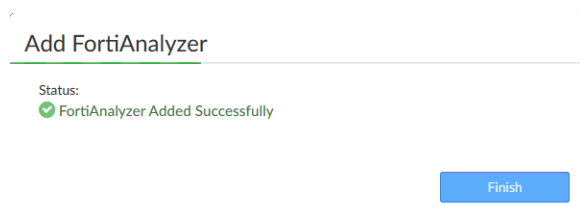
If the FortiManager ADOM does not exist on the FortiAnalyzer device, a warning is displayed. You can add the ADOM and devices to FortiAnalyzer by clicking the *Synchronize ADOM and Devices* button.

7. Click *Synchronize ADOM and Devices* to continue.

- a. If you are synchronizing devices from FortiAnalyzer to FortiManager, type the IP address and login for each device, and click *OK* to synchronize the devices.
- b. After the devices successfully synchronize, click *OK* to continue.

The devices, ADOM name, and ADOM version are synchronized between FortiAnalyzer and FortiManager.

8. Click *Finish* to close the wizard.



The FortiAnalyzer device is displayed on the *Device Manager* pane as a *Managed FortiAnalyzer*, and FortiAnalyzer features are enabled.

After completing the wizard, ensure that you enable logging on the devices, so the managed FortiAnalyzer can receive logs from the devices. You can enable logging by using the log settings in a system template. See [System templates on page 155](#).

Importing devices

You can import devices using the following methods:

- [Importing detected devices](#)
- [Importing and exporting device lists](#)

Importing detected devices

You can import detected devices for each device.

To import detected devices:

1. Ensure that you are in the correct ADOM.
2. Go to the *Device Manager* tab, and from the *Tools* menu, click *Global Display Options*.
3. In the *Detected Devices* area, select *Detected Devices*, and click *OK*.
4. In the tree menu, select a device. The device dashboard is displayed.

5. Click *Detected Devices*. The *Detected Devices* pane is displayed.
6. Click *Import*.

Importing and exporting device lists

Using the *Import Device List* and *Export Device List* function, you can import or export a large number of devices, ADOMs, device VDOMs, and device groups. The device list is a compressed text file in JSON format.



Advanced configuration settings such as dynamic interface bindings are not part of import/export device lists. Use the backup/restore function to backup the FortiManager configuration.



The *Import and Export Device List* features are disabled by default. To enable, go to *System Settings > Admin > Admin Settings*, and select the *Show Device List Import/Export* checkbox under *Display Options on GUI*.



Proper logging must be implemented when importing a list. If any add or discovery operation fails, there must be appropriate event logs generated so you can trace what occurred.

You can create the compressed text file by exporting a device list from FortiManager.

To export a device list:

1. Go to *Device Manager > Device & Groups*.
2. Select a device group, such as *Managed FortiGates*.
3. From the *More* menu, select *Export Device List*.
A device list in JSON format is exported in a compressed file (`device_list.dat`).

To import a device list:

1. Go to *Device Manager > Device & Groups*.
2. Select a device group, such as *Managed FortiGates*.
3. From the *More* menu, select *Import Device List*.
4. Click *Browse* and locate the compressed device list file (`device_list.dat`) that you exported from FortiManager, or drag and drop the file onto the dialog box.
5. Click *OK*.

Configuring devices

You can configure the FortiGate units in three ways:

- Per device, from the Device Manager dashboard toolbar.
- Per VDOM, from the Device Manager dashboard toolbar.
- Per provisioning template.

This section contains the following topics:

- [Configuring a device](#)
- [Out-of-Sync device](#)
- [Configuring VDOMs](#)

Configuring a device

Configuring a FortiGate unit using the *Device Manager* dashboard toolbar is very similar to configuring FortiGate units using the FortiGate GUI. You can also save the configuration changes to the configuration repository and install them to other FortiGate units at the same time.

This document does not provide detailed procedures for configuring FortiGate units. See the FortiGate documentation for complete information. The most up-to-date FortiGate documentation is also available in the [Fortinet Document Library](#).

To configure a FortiGate unit:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the content pane, select a device.
4. From the *Install* menu, select *Install Config*.
5. When the installation configuration is complete, click *Finish*.

The configuration changes are saved to the FortiManager device database instead of the FortiManager repository represented by the *Revision History* window.



To view the history of the configuration installation, click the *View History* button in the *History* column to open the *Install History* dialog box. This can be particularly useful if the installation fails.



You can rename and reapply firewall objects after they are created and applied to a firewall policy. When you do so, the FortiManager system will: delete all dependencies, delete the object, recreate a new object with the same value, and recreate the policy to reapply the new object.

Firewall policy reordering on first installation

On the first discovery of a FortiGate unit, the FortiManager system will retrieve the unit's configuration and load it into the Device Manager. After you make configuration changes and install them, you may see that the FortiManager system reorders some of the firewall policies in the FortiGate unit's configuration file.

This behavior is normal for the following reasons:

- The FortiManager system maintains the order of policies in the actual order you see them and manipulate them in the GUI, whereas the FortiGate unit maintains the policies in a different order (such as order of creation).

- When loading the policy set, the FortiManager system re-organizes the policies according to the logical order as they are shown in the user interface. In other words, FortiManager will group all policies that are organized within interface pairs (internal -> external, port1 -> port3, etc.).

The FortiManager system does not move policies within interface pairs. It will only move the configuration elements so that policies with the same source/destination interface pairs are grouped together.

This behavior would only be seen:

- On the first installation.
- When the unit is first discovered by the FortiManager system. If using the FortiManager system to manage the FortiGate unit from the start, you will not observe the policy reordering behavior.

Out-of-Sync device

FortiManager is able to detect when the settings were changed on the FortiGate and synchronize back to the related policy and object settings. This allows you to know when the policy package is out-of-sync with what is installed on the FortiGate.

When a change is made to the FortiGate, FortiManager displays an out-of-sync dialog box.

Select the *View Diff* icon to view the changes between the FortiGate and FortiManager.

You can select to accept, revert the modification, or decide later.



When accepting remote changes, all local configurations will be replaced by remote configurations. When reverting, the FortiGate will be reset to the latest revision.

You can view details of the retrieve device configuration action in the Task Monitor. See [Task Monitor on page 508](#).



If connectivity is down, the indicated configuration status might be incorrect. When connectivity is reestablished, a configuration checksum will be performed and the status will be updated.

Configuring VDOMs

Virtual domains (VDOMs) enable you to partition and use your FortiGate unit as if it were multiple units. For more information see the [FortiOS Handbook](#) available in the [Fortinet Document Library](#).



VDOMs have their own dashboard and toolbar. You can configure the VDOM in the same way that you can configure a device.

Delete

Select to remove this virtual domain. This function applies to all virtual domains except the root.

Create New	Select to create a new virtual domain.
Management Virtual Domain	Select the management VDOM and select <i>Apply</i> .
Name	The name of the virtual domain and if it is the management VDOM.
Virtual Domain	Virtual domain type.
IP/Netmask	The IP address and mask. Normally used only for Transparent mode.
Type	Either VDOM Link or Physical.
Access	HTTP, HTTPS, SSH, PING, SNMP, and/or TELNET.
Resource Limit	Select to configure the resource limit profile for this VDOM.

Creating and editing virtual domains

Creating and editing virtual domains in the FortiManager system is very similar to creating and editing VDOMs using the FortiGate GUI.

You need to enable virtual domains before you can create one.

To enable virtual domains:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the lower tree menu, select a device. The device dashboard displays.
4. In the *System Information* widget, select the *Enable* link in the *VDOM* field.

To create a virtual domain:

1. In the *Device Manager* tab, display the device dashboard for the unit you want to configure.
2. From the *System* menu, select *Virtual Domain*.
3. Click *Create New* to create a new VDOM.



The Virtual Domain tab may not be visible in the content pane tab bar. See [View system dashboard for managed/logging devices on page 129](#) for more information.

After the first VDOM is created you can create additional VDOMs by right-clicking on the existing VDOM and selecting *Add VDOM* from the right-click menu.

4. Complete the options, and click *OK* to create the new VDOM.

Configuring inter-VDOM routing

By default, for two virtual domains to communicate it must be through externally connected physical interfaces. Inter-VDOM routing creates a link with two ends that act as virtual interfaces, internally connecting the two virtual domains.

Before configuring inter-VDOM routing:

- You must have at least two virtual domains configured.
- The virtual domains must all be in NAT mode.
- Each virtual domain to be linked must have at least one interface or subinterface assigned to it.

To create a VDOM link:

1. In the *Device Manager* pane, display the device dashboard for the virtual domain.
2. From the *System* menu, select *Interface*.
3. Click *Create New > VDOM Link*. The *New VDOM Link* pane opens.

New VDOM Link

Name

Interface #0

VDOM

IP/Netmask

Administrative Access ☐ HTTP ☐ HTTPS ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ TELNET

Description (63 characters)

Interface #1

VDOM

IP/Netmask

Administrative Access ☐ HTTP ☐ HTTPS ☐ PING ☐ FMG-Access
☐ SSH ☐ SNMP ☐ TELNET

Description (63 characters)

4. Enter the following information:

Name	Name of the VDOM link.
Interface #x	The interface number, either <i>1</i> or <i>0</i> .
VDOM	Select the VDOM
IP/Netmask	Type the IP address and netmask for the VDOM.
Administrative Access	Select the allowed administrative service protocols from: HTTPS, HTTP, PING, SSH, Telnet, SNMP, and Web Service.
Description	Optionally, type a description for the link.

5. Click *OK* to save your settings.

Deleting a virtual domain

Prior to deleting a VDOM, all policies must be removed from the VDOM. To do this, apply and install a blank, or empty, policy package to the VDOM (see [Create new policy packages on page 217](#)). All objects related to the VDOM must also be removed, such as routes, VPNs, and admin accounts.

To delete a VDOM:

1. In the *Device Manager* tab, display the device dashboard for the unit you want to configure.
2. From the *System* menu, select *Virtual Domain*.

3. Right-click on the VDOM and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the VDOM.

Using the device dashboard

You can view the dashboard and related information of all managed/logging and provisioned devices.

This section contains the following topics:

- [View system dashboard for managed/logging devices](#)
- [View system interfaces on page 131](#)
- [CLI-Only Objects menu](#)
- [System dashboard widgets](#)

View system dashboard for managed/logging devices

You can view information about individual devices in the *Device Manager* pane on the dashboard for each device. This section describes the dashboard for a FortiGate unit.

To view the dashboard for managed/logging devices:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed FortiGates*. The list of devices display in the content pane and in the bottom tree menu.



When the FortiAnalyzer feature set is enabled, the *All FortiGates* device group is replaced with *Managed FortiGates* and *Logging FortiGates*. Managed FortiGates include FortiGate devices, which are managed by FortiManager but do not send logs. Logging FortiGates include FortiGate devices which are not managed, but do send logs to FortiManager.

3. In the bottom tree menu, select a device. The *System: Dashboard* for the device displays in the content pane.

The screenshot shows the FortiManager interface for a specific device. The top navigation bar includes tabs for Router, WAN Opt. & Cache, Security Profiles, VPN, Wireless, Query, Detected Devices, CLI-Only Objects, and Display Options. The main content area is titled 'System: Dashboard' and contains the following sections:

- System Information:** A table listing device details such as Host Name, Serial Number, System Time, Firmware Version, Hardware Status, Operation Mode, Inspection Mode, HA Mode, Session Information, Description, and Operation (with Reboot and Shutdown buttons).
- License Information:** A section for VM License and Support Contract, showing license status, resources, registration, and support expiration dates.
- Connection Summary:** A table showing IP, Interface, Connecting User, Connectivity, and Connect to CLI via options.
- Configuration and Installation Status:** A section showing System Template, Database Configuration, Total Revisions, Sync Status, Warning, Installation Tracking, Device Settings Status, Installation Preview, Last Installation, Scheduled Installation, Script Status, Last Script Run, and Scheduled Script.

4. In the dashboard toolbar, click the tabs to display different options that you can configure for the device. See [Dashboard toolbar on page 130](#).
- For information on configuring FortiGate settings locally on your FortiManager device, see the *FortiOS Handbook*.
5. You can control what tabs are displayed by clicking *Display Options*. See [Display Options on page 130](#).

Dashboard toolbar

The dashboard toolbar displays tabs that you can use to configure the device. The available tabs depends on the device. You can choose what tabs to display by clicking display options.



The options available on the dashboard toolbar varies depending on what feature set the device supports. If a feature is not enabled on the device the corresponding tab is not available on the toolbar.

Display Options

You can customize panels at both the ADOM and device levels. Select *Tools > Display Options* to open the *Display Options* dialog box to customize the available content at the ADOM level. Alternatively, you can select a device, and then select *Display Options* to customize device tabs. You can select to inherit from ADOM or customize.



The options available when customizing device tabs at the ADOM level will vary based on the ADOM version.

To select all of the content panels in a particular category, select the checkbox beside the category name. To reset a category selection, clear the checkbox.

To select all of the content panels, select *Check All* at the bottom of the window. To reset all of the selected panels, select *Reset to Default* at the bottom of the window.



The available device tabs are dependent on the device model and settings configured for that model. The following tables provide an overview and descriptions of common dashboard toolbar panels, and content options.

View system interfaces

You can view interface information about individual devices in the *Device Manager* tab.

To view interfaces for a device:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed FortiGates*. The list of devices is displayed in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select a device. The dashboard for the device displays in the content pane.
4. From the *System* menu, select *Interface*. The *System: Interface* dashboard is displayed.

CLI-Only Objects menu

FortiManager includes a *CLI-Only Objects* menu in the *Device Manager* pane that allows you to configure device settings that are normally configured via the CLI on the device, as well as settings that are not available in the FortiManager GUI.

To access the CLI-only objects menu:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select a device group.
3. In the lower tree menu, select a device. The device dashboard is displayed in the content pane.
4. Click *Display Options*. The *Display Options* dialog box is displayed.
5. Select the *CLI-Only Objects* checkbox, and click *OK*. The *CLI-Only Objects* menu is displayed in the toolbar.
6. Click *CLI-Only Objects*.



The options available in the menu will vary from device to device depending on what feature set the device supports. The options will also vary depending on the device firmware version.

System dashboard widgets

The system dashboard widgets provide quick access to device information, and device connectivity with the FortiManager system. The following widgets are available in FortiManager:

- [System Information](#)
- [License Information](#)
- [Connection Summary](#)
- [Configuration and Installation Status](#)

The following table provide a description of these dashboard widgets. Note that not all of the listed options will be available on every device.

System Information	
Host Name	The host name of the device.
Serial Number	The device serial number.
System Time	The device system time and date information.
Firmware Version	The device firmware version and build number.
Hardware Status	The number of CPUs and the amount of RAM for the device.
Operation Mode	Displays whether the device is in <i>NAT</i> or <i>Central NAT</i> operation mode.
Inspection Mode	Displays whether the device is in <i>Proxy</i> or <i>Flow-Based</i> inspection mode.
HA Mode	FortiGate HA configuration on FortiManager is read-only. Standalone indicates non-HA mode. Active-Passive, Active-Active indicates the device is operating in a cluster.
VDOM	The status of VDOMs on the device.
Session Information	Select <i>View Session List</i> to view the device session information.
Description	Descriptive information about the device.
Operation	Select <i>Reboot</i> to reboot the device or <i>Shutdown</i> to shut down the device.
License Information	
VM License	The VM license information.
Support Contract	The support contract information and the expiry date. The support contract includes the following: Registration, Hardware, Firmware, and Support Level e.g. Enhanced Support, Comprehensive Support.
FortiGuard Services	The contract version, issue date and service status. FortiGuard Services includes the following: Antivirus, Intrusion protection, Web filtering, and Email filtering.
VDOM	The number of virtual domains that the device supports.
Connection Summary	
IP	The IP address of the device.
Interface	The port used to connect to the FortiManager system.

Connection Summary

Connecting User	The user name for logging in to the device.
Connectivity	<p>The device connectivity status and the time it was last checked. A green arrow means that the connection between the device and the FortiManager system is up; a red arrow means that the connection is down.</p> <p>Select <i>Refresh</i> to test the connection between the device and the FortiManager system.</p>
Connect to CLI via	Select the method by which you connect to the device CLI, either SSH or TELNET.

Configuration and Installation Status

System Template	The system template associated with the device. Select <i>Change</i> to set this value.
Database Configuration	Select <i>View</i> to display the configuration file of the FortiGate unit.
Total Revisions	<p>Displays the total number of configuration revisions and the revision history.</p> <p>Select <i>Revision History</i> to view device history. Select the revision history icon to open the <i>Revision Diff</i> menu. You can view the diff from a previous revision or a specific revision and select the output.</p>
Sync Status	<p>The synchronization status with the FortiManager:</p> <ul style="list-style-type: none"> • <i>Synchronized</i>: The latest revision is confirmed as running on the device. • <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system. • <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. <p>Select <i>Refresh</i> to update the Installation Status.</p>
Warning	<p>Displays any warnings related to configuration and installation status:</p> <ul style="list-style-type: none"> • <i>None</i>: No warning. • <i>Unknown configuration version running on FortiGate: FortiGate configuration has been changed!</i>: The FortiManager system cannot detect which revision (in <i>Revision History</i>) is currently running on the device. • <i>Unable to detect the FortiGate version</i>: Connectivity error! • <i>Aborted</i>: The FortiManager system cannot access the device.

Installation Tracking

Device Settings Status	<ul style="list-style-type: none"> • <i>Modified</i>: Some configuration on the device has changed since the latest revision in the FortiManager database. Select <i>Save Now</i> to install and save the configuration. • <i>UnModified</i>: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Select the icon to display a set of commands that will be used in an actual device configuration installation in a new window.

Configuration and Installation Status

Last Installation	The FortiManager system sent a configuration to the device at the indicated date and time.
Scheduled Installation	A new configuration will be installed on the device at the indicated date and time.
Script Status	Select Configure to view script execution history.
Last Script Run	Displays the date when the last script was run against the managed device.
Scheduled Script	Displays the date when the next script is scheduled to run against the managed device.



The information presented in the System Information, License Information, Connection Summary, and Configuration and Installation Status widgets will vary depending on the managed device model.

Installing to devices

- To use the *Install Wizard* to install policy packages and device settings to one or more FortiGate devices, see [Using the Install Wizard to install policy packages and device settings on page 134](#).
- To use the *Install Wizard* to install device settings only, see [Using the Install Wizard to install device settings only on page 136](#).
- To reinstall a policy package without using the *Install Wizard*, see [Reinstall a policy package on page 221](#).

Using the Install Wizard to install policy packages and device settings

You can use the *Install Wizard* to install policy packages and device settings to one or more FortiGate devices, including any device-specific settings for the devices associated with that package.

To use the Install Wizard to install policy packages and device settings:

1. If using ADOMs, ensure you are in the correct ADOM.
2. In the toolbar, select *Install Wizard* or *Install > Install Wizard*.
3. Select *Install Policy Package & Device Settings* and specify the policy package and other parameters. Click *Next*.

Install Wizard

☒ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: default

Comment: Write a comment

☒ **Create ADOM Revision**

Revision Name: default_2017-7-17-15-14-10

Revision Comments: Write a comment

☒ **Schedule Install**

2017/07/17 03:14 PM

☐ **Install Device Settings (only)**

Next > Cancel

Policy Package	Select the policy package from the dropdown list.
Comment	Type an optional comment.
Create ADOM Revision	Select the checkbox to create an ADOM revision.
Revision Name	Type the revision name.
Revision Comments	Type an optional comment.
Schedule Install	Select the checkbox to schedule the installation.
Date	Click the date field and select the date for the installation in the calendar pop-up.
Time	Select the hour and minute from the dropdown lists.

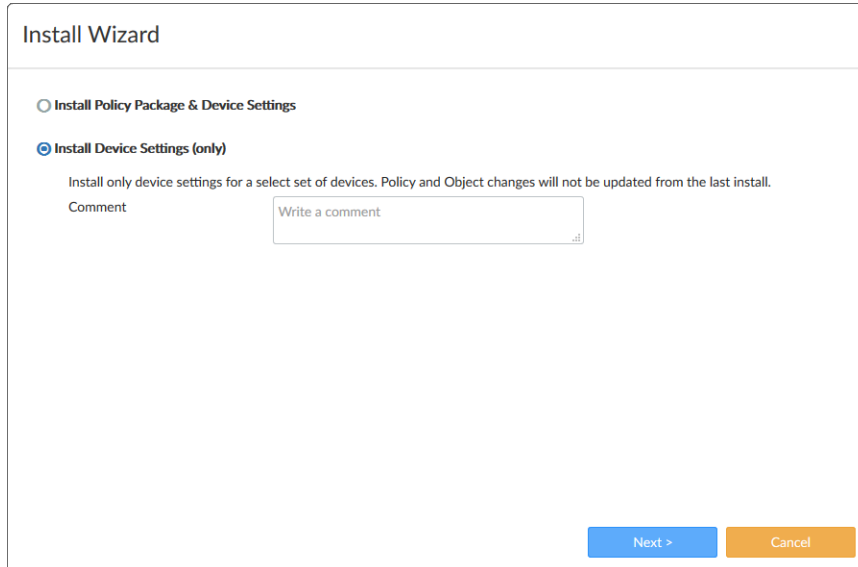
- On the next page, select one or more devices or groups to install, and click *Next*.
The select devices are validated. Validation includes validating the policy and object, the interface, and installation preparation. Devices with validation errors are skipped for installation. The validation results are displayed.
- (Optional) Click the *Install Preview* button to view a preview of the installation and download a text file of the installation preview details. You can also download a text file of the installation preview details.
- (Optional) Click the *Policy Package Diff* button to view the differences between the current policy and the policy in the device. See also [View a policy package diff on page 136](#).
- When validation is complete, click *Install* or *Schedule Install* (if you selected *Schedule Install*).
FortiManager displays the status of the installation and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.
- Click *Finish* to close the wizard.

Using the Install Wizard to install device settings only

You can use the *Install Wizard* to install device settings only to one or more FortiGate devices. The *Install Wizard* includes a preview feature.

To use the Install Wizard to install device settings only:

1. If using ADOMs, ensure you are in the correct ADOM.
2. In the toolbar, select *Install Wizard* or *Install > Install Wizard*.
3. Select *Install Device Settings (only)* and if you want, type a comment. Click *Next*.



4. In the *Device Settings* page, select one or more devices to install, and click *Next*.
5. (Optional) Preview the changes:
 - a. Click *Install Preview*.
The *Install Preview* window is displayed. You have the option to download a text file of the settings.
 - b. Click *Close* to return to the installation wizard.
6. Click *Install*.
FortiManager displays the status of the installation and then lists the devices onto which the settings were installed and any errors or warning that occurred during the installation process.
You can click the *View History* and *View Log* buttons for more information.
7. Click *Finish* to close the wizard.

View a policy package diff

You can view the difference between the policy package associated with (or last installed on) the device and the policies and policy objects in the device.

The connection to the managed device must be up to view the policy package diff.

To view a policy package diff in *Device Manager*:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. Right-click a device and select *Policy Package Diff*.
The *Policy Package Diff* window is displayed after data is gathered.

The screenshot shows the 'Policy Package Diff (p1)' window. It has a 'Summary' tab selected. The window displays two tables of changes.

Policy - added (1) [Details]

Category	Change Summary	User	
IPv4 Policy	added (1)	admin	[Details]

Policy Object - added (5) changed (3) deleted (106) [Details]

Category	Change Summary	User	
CA Certificate	added (1)	admin	
Local User	deleted (1)	admin	
User Group	deleted (1)	admin	
Device Group	deleted (3)	admin	
Local Category	deleted (2)	admin	
Web Filter Profile	changed (1) deleted (4)	admin	
Address	added (1) changed (1) deleted (1)	admin	
Multicast Address	deleted (5)	admin	
IPv6 Address	deleted (1)	admin	

A 'Close' button is located at the bottom right of the window.

4. Beside *Policy*, click the *Details* link to display details about the policy changes.
5. In the *Category* row, click the *Details* link to display details about the specific policy changes.
6. Beside *Policy Object*, click the *Details* link to display details about the policy object changes.
7. Click *Cancel* to close the window.

Managing devices

Once a device has been added to the *Device Manager* pane, the configuration is available within other tabs in the FortiManager system, such as *Policy & Objects*.

This section includes the following topics:

- [Using the quick status bar](#)
- [Customizing columns](#)
- [Refreshing a device](#)
- [Editing device information](#)
- [Replacing a managed device](#)
- [Setting unregistered device options](#)
- [Using the CLI console for managed devices](#)

Using the quick status bar

You can quickly view the status of devices on the *Device Manager* pane by using the quick status bar, which contains the following information:

- Devices Total
- Devices Connection
- Devices Device Config
- Devices Policy Package

You can click each quick status to display only the devices referenced in the quick status.

To view the quick status bar:

1. Go to *Device Manager > Device & Groups*. The quick status bar is displayed.



2. In the tree menu, select a group. The devices for the group are displayed in the content pane, and the quick status bar updates.
3. Click the menu on each quick status to filter the devices displayed on the content pane.
For example, click the menu for *Device Config* and select *Modified*. The content pane displays only devices in the selected group with modified configuration files.
4. Click *Devices Total* to return to the main view.

Customizing columns

You can choose what columns display on the content pane for the *Device Manager > Device & Groups* pane.

Column settings are not available for all device types. The default columns also vary by device type.

You can filter columns that have a *Filter* icon. Column filters are not available for all columns.



The columns available in the *Column Settings* menu depends on features enabled in FortiManager. When the FortiAnalyzer feature set is disabled, all related settings are hidden in the GUI.

To customize columns:

1. Go to *Device Manager > Device & Groups*.
2. Click *Column Settings* and select the columns you want to display.

Refreshing a device

Refreshing a device refreshes the connection between the selected devices and the FortiManager system. This operation updates the device status and the FortiGate HA cluster member information.

To refresh a device:

1. In the content pane, select a device.
2. Select *More > Refresh Device*. The *Update Device* dialog box opens to show the refresh progress.

Editing device information

Use the *Edit Device* page to edit information about a device. The information and options available on the *Edit Device* page depend on the device type, firmware version, and which features are enabled. Some settings only display when the FortiAnalyzer feature set is enabled.

To edit information for a device or model device:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group.
3. In the content pane, select the device or model device, and click *Edit*. The *Edit Device* pane displays.

Edit Device

Name	<input type="text" value="FG"/>
Description	<input type="text"/>
Company/Organization	<input type="text"/>
Country	<input type="text"/>
Province/State	<input type="text"/>
City	<input type="text"/>
Contact	<input type="text"/>
Geographic Coordinates	
Latitude	<input type="text" value="0"/>
Longitude	<input type="text" value="0"/>
IP Address	<input type="text"/>
Automatically link to real device	<input checked="" type="checkbox"/>
Admin User	<input type="text"/>
Password	<input type="password"/>
Device Information:	
Serial Number	FGVMEV0000000005
Device Model:	FortiGate-VM
Firmware Version:	FortiGate 5.4/build1007
Connected Interface:	
HA Mode	Unknown
Device Permissions	<input checked="" type="checkbox"/> Logs <input checked="" type="checkbox"/> DLP Archive <input checked="" type="checkbox"/> Quarantine <input checked="" type="checkbox"/> IPS Packet Log

4. Edit the device settings as required.

Name	The name of the device.
Description	Descriptive information about the device.
Company/Organization	Company or organization information.
Country	Type the country.
Province/State	Type the province or state.
City	Type the city.
Contact	Type the contact information.
Geographic Coordinates	Identifies the latitude and longitude of the device location to support the interactive maps.
IP Address	The IP address of the device.
Pre-Shared Key	The model device's pre-shared key. Select <i>Show Pre-shared Key</i> to see the key. This option is only available when editing a model device that was added with a pre-shared key.
Automatically link to real device	Automatically register the device with FortiManager when the device is online. This option is not available for FortiAnalyzer devices.
Admin User	The administrator user name.
Password	The administrator user password.
Device Information	Information about the device, including some or all of: serial number, device model, firmware version, connected interface, HA mode, cluster name, and cluster members.
Secure Connection	Select to enable a secure connection to the FortiGate device. Include the ID for the device and a pre-shared key.
HA Mode	Displays whether the FortiGate unit is operating in standalone or high availability mode.
Device Permissions	Specify the permissions for the FortiGate device. Select <i>Logs</i> , <i>DLP Archive</i> , <i>Quarantine</i> , or <i>IPS Packet Log</i> .

5. After making the appropriate changes click *OK*.

Enable *Secure Connection* to secure OFTP traffic over IPsec. Enabling *Secure Connection* increases the load on FortiManager. This feature is disabled by default.



In an HA environment, if you enable *Secure Connection* on one cluster member, you must enable *Secure Connection* on all cluster members.

Deleting a device

Devices can be deleted in Device Manager. Deleting a device does not delete other management elements associated with it:

- If the device is a member of a group, the group will remain without the device in it ([Device groups on page 150](#)).
- If a template is assigned to the device, the template will remain with no device assignment ([Provisioning Templates on page 155](#)).
- If the device is an installation target for a policy package, the package will remain with that device removed from the installation targets ([Policy package installation targets on page 224](#)).
- If there is a policy in a policy package that only installs on the device that is deleted, the policy will remain but will not be installed on any devices (see [Install policies only to specific devices on page 233](#)).
- If there are VDOMs in other ADOMs, they will be deleted with the device ([ADOM device modes on page 55](#)).

To delete a device:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager > Device & Groups*.
3. In the content pane, select a device and then click *Delete* in the toolbar, or right click on a device and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the device.

Replacing a managed device

The serial number is verified before each management connection. If you replace a device, you must manually change the serial number in the FortiManager system and re-deploy the configuration.



You can only reinstall a device that has a *Retrieve* button under the *Revision History* tab.

View all managed devices from the CLI

To view all devices that are managed by your FortiManager, use the following command:

```
diagnose dvm device list
```

The output lists the number of managed devices, device type, OID, device serial number, VDOMs, HA status, IP address, device name, and the ADOM to which the device belongs.

Changing the serial number from the CLI

If the device serial number was entered incorrectly using the *Add Model Device* wizard, you can replace the serial number from the CLI only. Use the command:

```
execute device replace sn <device name> <serial number>
```

This command is also useful when performing an RMA replacement.

Setting unregistered device options

In 5.2, setting unregistered device options is from the CLI only. Type the following command lines to enable or disable allowing unregistered devices to be registered with the FortiManager.

```
config system admin setting
  set allow_register [enable | disable]
  set unreg_dev_opt add_allow_service
  set unreg_dev_opt add_no_service
end
```

allow_register [enable disable]	When the <code>set allow_register</code> command is set to <code>enable</code> , you will not receive the unregistered device dialog box.
unreg_dev_opt	Set the action to take when an unregistered device connects to FortiManager.
add_allow_service	Add unregistered devices and allow service requests.
add_no_service	Add unregistered devices but deny service requests.



When the `set allow_register` command is set to `disable`, you will not receive the unregistered device dialog box.

Using the CLI console for managed devices

You can access the CLI console of managed devices.

To use the CLI console:

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and in the bottom of the tree menu, select a device. The device dashboard displays.
3. On the *Connection Summary* widget *Connect to CLI via* line, select *TELNET* or *SSH*.

Connect to:	Shows the device that you are currently connected to. Select the dropdown menu to select another device.
IP	The IP address of the connected device.
Telnet SSH	Connect to the device via Telnet or SSH.
Connect Disconnect	Connect to the device you select, or terminate the connection.
Close	Exit the CLI console.

You can cut (*CTRL+C*) and paste (*CTRL+V*) text from the CLI console. You can also use *CTRL+U* to remove the line you are currently typing before pressing *ENTER*.

Displaying security fabric topology

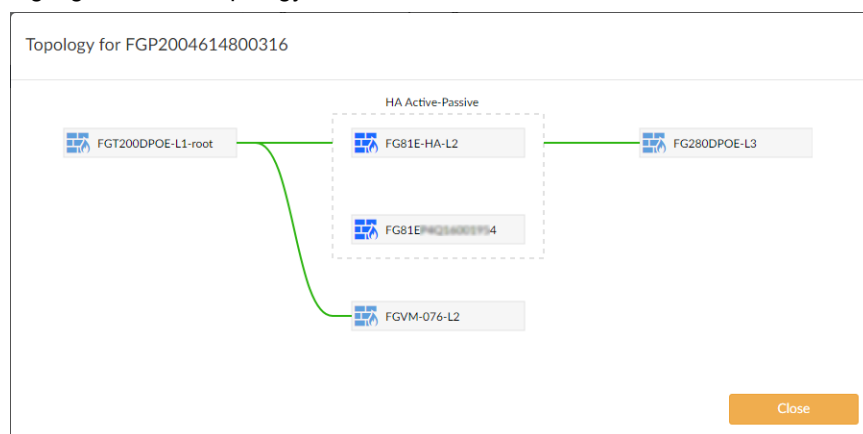
For security fabric devices, you can display the security fabric topology.

To display the security fabric topology:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Device Manager* and click the *Devices Total* tab in the quick status bar.
3. Right-click a security fabric device and select *Fabric Topology*.

A pop-up window displays the security fabric topology for that device.

If you selected *Fabric Topology* by right-clicking a device within the security fabric group, the device is highlighted in the topology. If you selected *Fabric Topology* by right-clicking the name of the security fabric group, no device is highlighted in the topology.



Managing device configurations

The FortiManager system maintains a configuration repository to manage device configuration revisions. After modifying device configurations, you can save them to the FortiManager repository and install the modified configurations to individual devices or device groups. You can also retrieve the current configuration of a device or revert a device's configuration to a previous revision.

This section contains the following topics:

- [View configurations for device groups](#)
- [Checking device configuration status](#)
- [Managing configuration revision history](#)

View configurations for device groups

You can view configuration information for devices in a group on the *Device Manager* tab.

To view configurations:


1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, click the device group name, for example, *Managed FortiGates*. The devices in the group are displayed in the content pane.

The following columns are displayed. You can filter columns that have a Filter icon.



Device Name	Name of the device
Config Status	See the table below for config status details.
Policy Package Status	See the table below for policy package status details.
Hostname	Available for managed devices. Displays the host name for the device.
IP Address	IP address of the device
Platform	Available for managed devices. Displays the platform of the device.
Description	Description of the device

The following table identifies the different available config statuses.

Config Status	Icon	Description
Synchronized	Green check ✓	Configurations are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ⚠	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
Auto-update	Green check ✓	Configurations modified on the managed device are auto synced to FortiManager.
Modified (recent auto-updated)	Yellow triangle ⚠	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X ✖	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X ✖	When one of the following happens: <ul style="list-style-type: none"> • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.

Config Status	Icon	Description
Unknown	Gray question mark 	When one of the following happens: <ul style="list-style-type: none"> • Connection goes down • No revision is generated, like added model device

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check 	Policies and objects are imported into FortiManager.
Synchronized	Green check 	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle 	Policies or objects are modified on FortiManager.
Out of Sync	Red X 	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark 	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle 	No policy package is imported or installed.

Checking device configuration status

In the *Device Manager* pane, when you select a device, you can view that device's basic information under the *device dashboard*. You can also check if the current configuration file of the device stored in the FortiManager repository is in sync with the one running on the device.

If you make any configuration changes to a device directly, rather than using the FortiManager system, the configuration on the device and the configuration saved in the FortiManager repository will be out of sync. In this case, you can re synchronize with the device by retrieving the configuration from the device and saving it to the FortiManager repository.

You can use the following procedures when checking device configuration status on a FortiGate, FortiCarrier, or FortiSwitch.

To check the status of a configuration installation on a FortiGate unit:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.

The *Configuration and Installation Status* widget shows the following information:

System Template	Displays the name of the selected system template. Click <i>Change</i> to change the system template.
Database Configuration	Click <i>View</i> to display the database configuration file of the FortiGate unit.
Total Revisions	Displays the total number of configuration revisions and the revision history. Click <i>Revision History</i> to view device history. For details, see Managing configuration revision history on page 147 . Click <i>Revision Diff</i> to compare revisions. For details, see Comparing different configuration files on page 149 .
Sync Status	The synchronization status with the FortiManager. <ul style="list-style-type: none"> • <i>Synchronized</i>: The latest revision is confirmed as running on the device. • <i>Out_of_sync</i>: The configuration file on the device is not synchronized with the FortiManager system. • <i>Unknown</i>: The FortiManager system is unable to detect which revision (in revision history) is currently running on the device. Click <i>Refresh</i> to update the synchronization status.
Warning	Displays any warnings related to configuration and installation status. <ul style="list-style-type: none"> • <i>None</i>: No warning. • <i>Unknown configuration version running on FortiGate: FortiGate configuration has been changed!</i>: The FortiManager system cannot detect which revision (in revision history) is currently running on the device. • <i>Unable to detect the FortiGate version</i>: Connectivity error. • <i>Aborted</i>: The FortiManager system cannot access the device.
Installation Tracking	
Device Settings Status	<ul style="list-style-type: none"> • <i>Modified</i>: Some configuration on the device has changed since the latest revision in the FortiManager database. Click <i>Save Now</i> to install and save the configuration. • <i>UnModified</i>: All configuration displayed on the device is saved as the latest revision in the FortiManager database.
Installation Preview	Click <i>Preview</i> to preview an actual device configuration installation, including any errors and warnings.
Last Installation	Displays the last installation's date, time, revision number, and the person who did the installation.
Scheduled Installation	Displays the data and time when a new configuration will be installed on the device.
Script Status	
Last Script Run	Displays the date and time when the last script was run. Click <i>View History</i> to see the script execution history.
Scheduled Script	Displays the date and time when the next script is scheduled to run.

Managing configuration revision history

The revision history repository stores all configuration revisions for a device. You can view the version history, view configuration settings and changes, import files from a local computer, compare different revisions, revert to a previous revision, and download configuration files to a local computer.

To view the revision history of a FortiGate unit:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*. The *Configuration Revision History* dialog box opens.

View Config	View the configuration for the selected revision.
View Install Log	View the installation log for the selected revision.
Revision Diff	Show only the changes or differences between two versions of a configuration file. For details, see Comparing different configuration files on page 149 .
Retrieve Config	View the current configuration running on the device. If there are differences between the configuration file on the device and the configuration file in the repository, a new revision is created and assigned a new ID number.
More	From the More menu, you can select one of the following: <ul style="list-style-type: none"> • Download Factory Default • Revert • Delete • Rename • Import Revision

The following information is displayed:

ID	The revision number. Double-click an ID to view the configuration file. You can also click <i>Download</i> to save the configuration file.
Date & Time	The time and date when the configuration file was created.
Name	A name assigned by the user to make it easier to identify specific configuration versions. You can rename configuration versions.
Created by	The name of the administrator account used to create the configuration file.
Installation	Display the status of the installation. <i>N/A</i> indicates that the revision was not sent to the device. The typical situation is that the changes were part of a later revision that was sent out to the device. For example, you make some changes and commit the changes. Now you have a revision called ID1. Then you make more changes and commit the changes again. Then you have a revision called ID2, which also includes the changes you made in revision ID1. If you install revision ID2, then the status of revision ID1 becomes <i>N/A</i> .

Comments

Display the comment added to this configuration file when you rename the revision.

To view the configuration settings on a FortiGate unit:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Select the revision, and click *View Config*. The *View Configuration* pane is displayed.
6. To download the configuration settings, click *Download*.
7. Click *Return* when you finish viewing.

To add a tag (name) to a configuration version on a FortiGate unit:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Right-click the revision, and select *Rename*.
6. Type a name in the *Tag (Name)* field.
7. Optionally, type information in the *Comments* field.
8. Click *OK*.

Downloading and importing a configuration file

You can download a configuration file and a factory default configuration file. You can also import a configuration file into the FortiManager repository.



You can only import a configuration file that is downloaded from the FortiManager repository, otherwise the import fails.

To download a configuration file:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Select the revision you want to download.
6. Click *View Config > Download*.
7. Select *Regular Download* or *Encrypted Download*. If you select *Encrypted Download*, type a password.
8. Click *OK*.

To download a factory default configuration file:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. In the toolbar, click *Download Factory Default*.

To import a configuration file from a local computer:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Right-click a revision and select *Import Revision*.
6. Click *Browse* and locate the revision file, or drag and drop the file onto the dialog box.
7. If the file is encrypted, select *File is Encrypted*, and type the password.
8. Click *OK*.

Comparing different configuration files

You can compare the changes or differences between two versions of a configuration file by using the *Diff* function.

The *Diff* function behaves differently under certain circumstances.

For example, when a device is first added to the FortiManager system, the FortiManager system gets the configuration file directly from the FortiGate unit and stores it as is. This configuration file is version/ID 1.

If you make changes to the device configuration in *Device Manager* and select *Commit*, the new configuration file is saved as version/ID 2. If you use the *Diff* icon to view the changes/differences between version/ID 1 and version/ID 2, you will be shown more changes than you have made.

This happens because the items in the file version/ID 1 are ordered as they are on the FortiGate unit. Configurations of version/ID 2 are sequenced differently when they are edited and committed in *Device Manager*. Therefore, when you compare version/ID 1 and version/ID 2, the *Diff* function sees every item in the configuration file as changed.

If you take version/ID 2, change an item and commit it, the tag is changed to version/ID 3. If you use *Diff* with version/ID 2 and version/ID 3, only the changes that you made are shown. This is because version/ID 2 and version/ID 3 have both been sequenced in the same way in *Device Manager*.

To compare different configuration files:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Select a revision, and click *Revision Diff* in the toolbar.
6. Select another version for the diff.

7. In the *Diff Output* section, select *Show Full File Diff*, *Show Diff Only*, or *Capture Diff to a Script*.
Show Full File Diff shows the full configuration file and highlights all configuration differences.
Show Diff Only shows only configuration differences.
Capture Diff to a Script downloads the diff to a script.
8. Click *Apply*.
If you selected show diff, the configuration differences are displayed in colored highlights. If you selected capture to a script, the script is saved in your downloads folder.

To revert to another configuration file:

1. Go to *Device Manager > Device & Groups* and select a device group.
2. In the lower tree menu, select a device. The content pane displays the device dashboard.
3. In the dashboard, locate the *Configuration and Installation Status* widget.
4. In the *Total Revisions* row, click *Revision History*.
5. Right-click the revision to which you want to revert, and click *Revert*.
The system immediately reverts to the selected revision.

Device groups

On the *Device Manager > Device & Groups* pane, you can create, edit, and delete device groups.

Default device groups

When you add devices to FortiManager, devices are displayed in default groups based on the type of device. For example, all FortiGate devices are displayed in the *Managed FortiGates* group. You can create custom groups.

Add device groups

You can create a group and add devices to the group.

To add device groups:

1. Go to *Device Manager > Device & Groups*.
2. From the *Device Group* menu, select *Create New*.
3. Complete the options, and click *OK*.

A group name can contain only numbers (0-9), letters (a-z, A-Z), and limited special characters (- and _).

Manage device groups

You can manage device groups from the *Device Manager > Device & Groups* pane. From the *Device Group* menu, select one of the following options:

Option	Description
Create New	Create a new device group.
Edit	Edit the selected device group. You cannot edit default device groups.
Delete	Delete the selected device group.



You must delete all devices from the group before you can delete the group. You must delete all device groups from an ADOM before you can delete an ADOM.

Firmware

On the *Device Manager > Firmware* pane, you can view the firmware installed on managed devices. You can also view whether a firmware upgrade is available and the upgrade history for devices.

View firmware for device groups

You can view firmware information for devices in a group.

To view firmware:

1. Go to *Device Manager*.
2. In the tree menu, select the device group name, for example, *Managed FortiGates*.
3. Click the *Firmware* tab.

For a description of the options, see [Firmware Management on page 152](#).

Upgrade firmware for device groups

The firmware of the devices within a group can also be updated as a group.

To update device group firmware:

1. Go to *Device Manager*.
2. In the tree menu, select the device group name, for example, *Managed FortiGates*.
3. Click the *Firmware* tab.
4. Locate an applicable firmware image in the *Available Upgrade* list, then click *Upgrade* to upgrade all of the devices in the group to that image.

The upgrade history is also shown and you can view more details by clicking *All History*.

Firmware Management

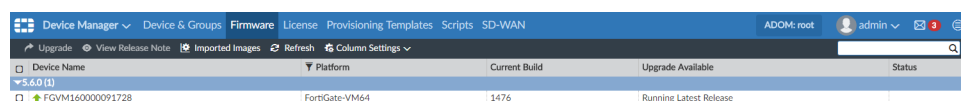
FortiGate device firmware can be updated from the *Device Manager > Firmware* pane. Upgrades can also be scheduled to occur at a later date.

The FortiGate device requires a valid firmware upgrade license. Otherwise a *Firmware Upgrade License Not Found* error is displayed.



When *Boot to Alternate Partition After Upgrade* is selected, the inactive partition will be upgraded.

In the *Device Manager* pane, select the *Managed FortiGates* group, then click the *Firmware* tab.



The following information and options are available:

Upgrade	Select to upgrade the selected device if the device can be upgraded.
View Release Notes	Select to view the release notes for the FortiOS version of the selected device.
Imported Images	Select to display the imported images where you can import or delete images.
Refresh	Refresh the list.
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
Device Name	The names of the FortiGate devices in the group, organized by firmware version.
Platform	The device platform.
Current Build	The build installed in the device.
Upgrade Available	The current firmware version and build number of the firmware on the device. If an update is available and can be applied to the device, Upgrade can be selected to open the <i>Upgrade Firmware</i> dialog box.
Status	The status of the device's license. If the license has expired, the firmware cannot be upgraded.
Upgrade History	Right-click a device and select <i>Show Upgrade History</i> to view the device's upgrade history.

To upgrade a device's firmware:

1. Go to *Device Manager*.
2. In the tree menu, select a device group, and then click the *Firmware* tab.
3. Select a device or device group with an upgrade available that is licensed for firmware upgrades, then click *Upgrade* in either the toolbar or in the *Upgrade Available* column. The *Upgrade Firmware* dialog box opens.

4. Configure the following settings, then click **OK**:

Upgrade to	Select a firmware version from the dropdown list.
Schedule Upgrade	Select to schedule the upgrade, then enter the date and time for the upgrade, and select an action to take if the update fails: <ul style="list-style-type: none"> • Cancel Upgrade • Retry: enter the number of times to retry and the time between retries.
Boot From Alternate Partition After Upgrade	Selecting this option causes the device to reboot twice during the upgrade process: first to upgrade the inactive partition, and second to boot back into the active partition.

License

On the *Device Manager > License* pane, you can view license information for managed devices.

View licenses for device groups

You can view license information for devices in a group.

To view licenses:

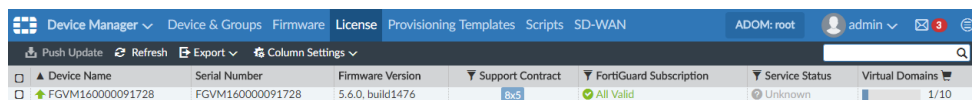
1. Go to *Device Manager*.
2. In the tree menu, select a device group, and then click the *License* tab.

For a description of the options, see [License Management on page 153](#).

License Management

You can check FortiGate device licenses in *Device Manager > License*.

In the *Device Manager* pane, select the *Managed FortiGates* group, then click the *License* tab.



The following columns are displayed. You can filter columns that have a *Filter* icon.

Device Name	Name of the device
Serial Number	Serial number for the device
Firmware Version	Firmware version for the device
Support Contract	<p>License status of the support contract. Hover over the license status to display expiration details about the following support contracts: hardware, firmware, enhanced support, and comprehensive support. License status can include:</p> <ul style="list-style-type: none"> • N/A: No support contract • 24/7: Support contract level that provides support 24 hours per day and 7 days per week • 8/5: Support contract level <p>Hover the mouse over the cell to display details about the support contract.</p>
FortiGuard Subscription	<p>License status of FortiGuard. The status reflects the worst license status of the individual components of the FortiGuard license. Hover over the license status to display details about the following components: IPS & Application Control, Antivirus, Web Filtering, and Email Filtering. License status can include:</p> <ul style="list-style-type: none"> • All valid • Expires in <time> • Expired • Unknown <p>Hover the mouse over the cell to display details about the FortiGuard subscription.</p>
Service Status	<p>License status of antivirus and IPS service:</p> <ul style="list-style-type: none"> • Update Available • Up to Date • Expired • Unknown <p>Hover the mouse over the cell to display details about the service status.</p>
Virtual Domains	<p>Number of virtual domains. Click the cart icon to go to the Fortinet support site (https://support.fortinet.com)</p>

The following buttons are available on the toolbar:

Push Update	Push a license update to the selected device in the group.
Refresh	Refresh the list of devices in the group.
Export	Click to export the device list, device update details, and license details to a PDF or CSV file format. A file in the selected format is downloaded to the management computer.
Column Settings	Click to select which columns display on the License pane.

Add-on license

Add-on licenses can be purchased for high end FortiManager devices to increase the number of device that can be managed. An add-on license can only be added using the CLI.

The below table lists the device that can have add-on licenses added, the number of devices the FortiManager can manage by default, and the maximum number of devices that can be managed by adding add-on licenses.

Model	Normal license	With add-on license
FMG-3900E	10000	100000
FMG-3000F	4000	8000
FMG-4000E	4000	8000

To add an add-on license:

1. Purchase an add-on license (<https://support.fortinet.com>).
2. Open the license file in a text editor.
3. Connect to the CLI and run the following command:

```
execute add-on-license <license>
```

Where `<license>` is the license text, copied and pasted from the text editor.
4. After the system automatically reboots, check the *License Information* widget to confirm that the number of *Devices/VODMs* that can be managed has increased. See [License Information widget on page 482](#).

Provisioning Templates

Go to *Device Manager > Provisioning Templates* to access configuration options for the following templates:

- [System templates](#)
- [Threat Weight templates](#)
- [Certificate templates](#)

System templates

The *Device Manager > Provisioning Templates > System Templates* pane allows you to create and manage device profiles. A system template is a subset of a model device configuration. Each device or device group can be linked with a system template. When linked, the selected settings come from the template and not from the Device Manager database.

By default, there is one generic profile defined. System templates are managed in a similar manner to policy packages. You can use the context menus to create new device profiles. You can configure settings in the widget or import settings from a specific device.

Go to the *Device Manager > Provisioning Templates > System Templates > default* pane to configure system templates.



System templates are available in 5.2, 5.4, and 5.6 ADOMs. Some settings may not be available in all ADOM versions.

After making changes in a widget, click *Apply* to save your changes.

To close a widget, click the *Close* icon in the widget's top right.

To select which widgets to display, click *Toggle Widgets* and select which widgets to display.

To import settings from another device, click the *Import* icon in the widget's top right and select the device from which to import.

The following widgets and settings are available:

Widget	Description
DNS	Primary DNS Server, Secondary DNS Server, Local Domain Name.
NTP Server	Synchronize with NTP Server and Sync Interval settings. You can select to use the FortiGuard server or specify one or more other servers.
Alert Email	SMTP Server settings including server, authentication, SMTP user ID, and password.
Admin Settings	Web Administration Ports, Timeout Settings, and Web Administration.
SNMP	SNMP v1/v2 and SNMP v3 settings. In the toolbar, you can select to create, edit, or delete the record. To create a new SNMP, click <i>Create New</i> and specify the community name, hosts, queries, traps, and SNMP events.
Replacement Messages	You can customize replacement messages. Click <i>Import</i> to select a device and the objects to import.

Widget	Description
Log Settings	You can select <i>Send Logs to FortiAnalyzer/FortiManager</i> and/or <i>Send Logs to Syslog</i> .
FortiGuard	Select <i>Enable FortiGuard Security Updates</i> to retrieve updates from FortiGuard servers or from this FortiManager. You can define multiple servers and specify <i>Update</i> , <i>Rating</i> , or <i>Updates and Rating</i> . You can also select <i>Include Worldwide FortiGuard Servers</i> .

You can create, edit, or delete templates. Select *System Templates* in the tree to display the *Create New*, *Edit*, *Delete*, and *Import* options in the content pane. You can also select the devices to be associated with the template by selecting *Assign to Device*.

To assign a system template to a device:

1. Go to *Device Manager > Provisioning Templates > System Templates*.
2. In the content pane, select a template and click *Assign to Device*.
3. Select devices to assign to and click *OK*.

The devices assigned to the template are shown in the *Assign to Device* column.

Threat Weight templates

User or client behavior can sometimes increase the risk of being attacked or becoming infected. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect that client, or a discussion with the user about this issue may be warranted.

Before you can decide on a course of action, you need to know the problem is occurring. Threat weight can provide this information by tracking client behavior and reporting on activities that you determine are risky or worth tracking.

Threat weight profiles can be created, edited, and assigned to devices. When Threat Weight Tracking is enabled, the *Log Allowed Traffic* setting is enabled on all policies. For more information on configuring the Threat Weight profile, see the *FortiOS Handbook*.

To create a new threat weight profile:

1. Go to the *Device Manager > Provisioning Templates > Threat Weight*.
2. Click *Create New* in the toolbar.
3. In the *Create New Threat Weight* pane, type a name for the profile.
4. Click *OK* to create the new threat weight profile.

To edit a threat weight profile:

1. Select a threat weight profile and click *Edit*. The *Edit Threat Weight* pane opens.
2. Adjust the threat levels as needed, then click *OK* to save your changes:

Log Threat Weight	Turn on threat weight tracking.
Reset	Reset all the threat level definition values to their defaults.

Import	Import threat level definitions from a device in the ADOM.
Application Protection	Adjust the tracking levels for the different application types that can be tracked.
Intrusion Protection	Adjust the tracking levels for the different attack types that can be tracked.
Malware Protection	Adjust the tracking levels for the malware or botnet connections that can be detected.
Packet Based Inspection	Adjust the tracking levels for failed connection attempts and traffic blocked by firewall policies.
Web Activity	Adjust the tracking levels for various types of web activity.
Risk Level Values	Adjust the values for the four risk levels.

To assign a threat weight profile to a device:

1. Select a threat weight profile and click *Assign to Device*.
2. Select devices to assign to and click *OK*.

The devices assigned to the template are shown in the *Assign to Device* column.

Certificate templates

The certificate templates menu allows you to create certificate templates for an external certificate authority (CA) or the local FortiManager CA.

FortiManager includes a certificate authority server for each ADOM. When you create an ADOM, the private and public key pair is created for the ADOM. The key pair is automatically used when you use FortiManager to define IPsec VPNs or SSL-VPNs for a device.

When you add a device to an IPsec VPN or SSL-VPN topology with a certificate template that uses the FortiManager CA, the local FortiManager CA is automatically used. No request for a pre-shared key (PSK) is generated. When the IPsec VPN or SSL-VPN topology is installed to the device, the following process completes automatically:

- The FortiGate device generates a certificate signing request (CSR) file.
- FortiManager signs the CSR file and installs the CSR file on the FortiGate device.
- The CA certificate with public key is installed on the FortiGate device.



Certificate templates are available in 5.0, 5.2, 5.4 and later ADOMs. Some settings may not be available in all ADOM versions.

The following options are available:

Create New	Create a new certificate template.
Edit	Edit a certificate template. Right-click a certificate template, and select <i>Edit</i> .

Delete	Delete a certificate template. Right-click a certificate template, and select <i>Delete</i> .
Generate	Create a new certificate from a device.

To create a new certificate template:

1. Go to *Device Manager > Provisioning Templates > Certificate Templates*.
2. Click *Create New*. The *Create New Certificate Template* pane opens.
3. Enter the following information, then click *OK* to create the certificate template:

Type	Specify whether the certificate uses an external or local certificate authority (CA). When you select <i>External</i> , you must specify details about online SCEP enrollment. When you select <i>Local</i> , you are using the FortiManager CA server.
Certificate Name	Type a name for the certificate.
Optional Information	Optionally, type the organization unit, organization, locality (city), province or state, country or region, and email address.
Key Type	RSA is the default key type. This field cannot be edited.
Key Size	Select the key size from the dropdown list: 512 bit, 1024 bit, 1536 bit, or 2048 bit.
Online SCEP Enrollment	
CA Server URL	Type the server URL for the external CA.
Challenge Password	Type the challenge password for the external CA server.

To edit a certificate template:

1. Select a certificate template, and click *Edit*.
2. Edit the settings as required in the *Edit Certificate Template* pane, and click *OK*.

To delete a certificate template:

1. Select a certificate template, and click *Delete*.
2. Click *OK* in the confirmation dialog box.

Scripts

FortiManager scripts enable you to create, execute, and view the results of scripts executed on FortiGate devices, policy packages, the ADOM database, the global policy package, or the DB. Scripts can also be filtered based on different device information, such as OS type and platform.

At least one FortiGate device must be configured in the FortiManager system for you to be able to use scripts.



Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes in the GUI page to access these options.



Any scripts that are run on the global database must use complete commands. For example, if the full command is `config system global`, do not use `conf sys glob`.

Scripts can be written in one of two formats:

- A sequence of FortiGate CLI commands, as you would type them at the command line. A comment line starts with the number sign (#). A comment line will not be executed.
- Tcl scripting commands to provide more functionality to your scripts including global variables and decision structures.

When writing your scripts, it is generally easier to write them in a context-sensitive editor, and then cut and paste them into the script editor on your FortiManager system. This can help avoid syntax errors and can reduce the amount of troubleshooting required for your scripts.

CLI scripts can be grouped together, allowing multiple scripts to be run on a target at the same time. See [CLI script group on page 166](#) for information.

For information about scripting commands, see the *FortiGate CLI reference*.



Before using scripts, ensure the `console-output` function has been set to `standard` in the FortiGate CLI. Otherwise, scripts and other output longer than a screen in length will not execute or display correctly.



When pushing a script from the FortiManager to the FortiGate with *workspace* enabled, you must save the changes in the *Policy & Objects* tab.

Enabling scripts

You must enable scripts to make the *Scripts* option visible in the GUI.

To enable scripts:

1. Go to *System Settings > Admin > Admin Settings*.
2. In the *Display Options on GUI* section, select *Show Scripts*. For more information, see [Global administration settings on page 98](#).
3. Select *Apply* to apply your changes.

Configuring scripts

To configure, import, export, or run scripts, go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM. The script list for your current ADOM displays.

The following information is displayed:

Name	The user-defined script name.
Type	The script type.
Target	The script target.
Comments	User defined comment for the script.
Last Modified	The date and time the script was last modified.

The following options are available in the toolbar, in the *More* menu, or in the right-click menu.

Run Script / Run	Run the selected script. See Run a script on page 161 .
Schedule Script	Schedule when the selected script will run. See Schedule a script on page 165 .
Create New / New	Create a new script. See Add a script on page 162 .
Edit	Edit the selected script. See Edit a script on page 164 .
Delete	Delete the selected script. See Delete a script on page 164 .
Clone	Clone the selected script. See Clone a script on page 164 .
Import CLI Script / Import	Import a script from your management computer. See Import a script on page 165 .
Export	Export the selected script as a <code>.txt</code> file to your management computer. See Export a script on page 164 .
Select All	Select all the scripts. This option is only available for Global Database scripts.
Search	Enter a search term in the search field to search the scripts.

Run a script

You can select to enable automatic script execution.

To run a script:

1. Go to *Device Manager > Scripts*.
2. Select the script, then right-click and select *Run* from the menu.



Scripts can also be re-run from the script execution history by selecting the run button. See [Script history on page 171](#) for information.

The *Execute Script* dialog box will open. This dialog box will vary depending on the script target. You will either be able to select a device or devices, or a policy package.

3. Select a device group or devices.
4. Select *OK* to run the script.

The *Run Script* dialog box will open, showing the progress of the operation and providing information on its success or failure.



Scripts can also be run directly on a device using the right-click menu in *Device Manager > Device & Groups*.

To run a script on the Global Database ADOM:

1. Go to *Policy & Objects > Object Configurations > Scripts*. If it is not visible, enable it in the *Display Options* ([Display options on page 216](#)).
2. Right-click a script and select *Run* from the menu. The *Execute Script* dialog box will open.
3. Select the policy package from the drop-down list.
4. Click *OK* to run the script.

The *Run Script* dialog box will open, showing the progress of the operation and providing information on its success or failure.

Add a script**To add a script to an ADOM:**

1. Go to *Device Manager > Scripts*, or *Policy & Objects > Object Configurations > Scripts* for the Global Database ADOM.
2. Click *Create New*, or right-click anywhere in the script list and select *New* from the menu. The *Create Script* dialog box.

Create New Script

Script Name

[View Sample Script]

Comments

0/255

Type

CLI Script

Run script on

Device Database

Script details

Advanced Device Filters >

OK

Return

3. Enter the required information, then click **OK** to create the new script.

Script Name	Type a unique name for the script.
View Sample Script	This option points to the FortiManager online help.
Comments	Optionally, type a comment for the script.
Type	Specify the type of script. This option is not available for Global Database ADOM scripts.
Run Script on	<p>Select the script target. This settings will affect the options presented when you go to run a script. The options include:</p> <ul style="list-style-type: none"> • <i>Device Database</i> • <i>Policy Package or ADOM Database</i> • <i>Remote FortiGate Directly (via CLI)</i> <p>For Global Database ADOM scripts, this option is set to <i>Policy Package or ADOM Database</i> and cannot be changed.</p>
Script Detail	Type the script itself, either manually using a keyboard, or by copying and pasting from another editor.
Advanced Device Filters	<p>Select to adjust the advanced filters for the script. The options include:</p> <ul style="list-style-type: none"> • <i>Platform</i> (select from the dropdown list) • <i>Build</i> • <i>Device</i> (select from the dropdown list) • <i>Host name</i> • <i>SN</i> <p>These options are not available for Global Database ADOM scripts, or if <i>Run script on</i> is set to <i>Policy Package or ADOM Database</i>.</p>

Edit a script

All of the same options are available when editing a script as when creating a new script, except the name of the script cannot be changed.

To edit a script, either double click on the script name, or right-click on the script name, then click *Edit* from the menu. The *Edit Script* dialog box will open, allowing you to edit the script and its settings. The script name and type cannot be changed.

Clone a script

Cloning a script is useful when multiple scripts that are very similar.

To clone a script:

1. Go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM.
2. Right-click a script, and select *Clone*.
The *Clone Script* pane opens, showing the exact same information as the original, except *copy_* is prepended to the script name.
3. Edit the script and its settings as needed then click *OK* to create the clone.

Delete a script

Scripts can be deleted from the script list as needed.

To delete a script or scripts:

1. Go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM.
2. Select the script to be deleted, or selected multiple scripts by holding down the Ctrl or Shift keys.
3. Right-click anywhere in the script list window, and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the script or scripts.

Export a script

Scripts can be exported to text files on your local computer.

To export a script:

1. Go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM.
2. Right-click a script, and select *Export*.
3. If prompted by your web browser, select a location to where save the file, or open the file without saving, then click *OK*.

Import a script

Scripts can be imported as text files from your local computer.

To import a script:

1. Go to *Device Manager > Scripts*.
2. Select *Import CLI Script* from the toolbar. The *Import CLI Script* window opens.
3. Drag and drop the script file onto the dialog box, or click *Add Files* and locate the file to be imported on your local computer.
4. Click *Import* to import the script.
If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be canceled.

To import a script in the Global Database ADOM:

1. Go to *Policy & Objects > Object Configuration > Advanced > Scripts*.
2. Select *Import* from the toolbar. The *Import Script* dialog box opens.
3. Enter a name for the script and, optionally, comments, in the requisite fields.
4. Click *Browse...* and locate the file to be imported on your local computer.
5. Click *Import* to import the script.
If the script cannot be read, due to an incorrect file type or other issue, an error message will be displayed and the import process will be canceled.

Schedule a script

Scripts and script groups can be scheduled to run at a specific time or on a recurring schedule. This option must be enabled in the CLI before it is available in the GUI.



Schedules cannot be used on scripts with the target *Policy Package* or *ADOM Database*.

To enable script scheduling:

1. Go to *System Settings > Dashboard* and click in the `CLI Console` widget, or connect to the FortiManager with terminal emulation software.
2. Enter the following CLI commands:

```
config system admin setting
  set show_schedule_script enable
end
```

To schedule a script or script group:

1. Go to *Device Manager > Scripts*, or *Policy & Objects > Object Configuration > Advanced > Scripts* if you are in the Global Database ADOM.

2. Right-click on the script or group and select *Schedule Script*, or select a script or group then click *Schedule Script* or *More > Schedule Script* in the toolbar. The *Schedule Script* window opens.
3. Configure the following options, then click *OK* to create the schedule:

Devices	Select the devices that the script will be run on. If required, use the search field to find the devices in the list.
Enable Automatic execute after each device install	Select to enable automatic execution of the script or script group after each device install. If this is selected, no schedule can be created. This option is only available is the target is <i>Remote FortiGate Directly (via CLI)</i> .
Enable Schedule	Select to schedule when the script or groups runs. This option is only available is the target is <i>Remote FortiGate Directly (via CLI)</i> .
Recurring	Select how frequently the script or script group will run: <ul style="list-style-type: none"> • <i>One Time</i>- Set the date and time that script or group will run. • <i>Daily</i> - Set the time that the script or group will run everyday. • <i>Weekly</i> - Set the day of the week and the time of day that the script or group will run. • <i>Monthly</i> - Set the day of the month and the time of day that the script or group will run.

CLI script group

CLI scripts can be put into groups so that multiple scripts can be run on a target at the same time.

To manage script groups, go to *Device Manager > Scripts > CLI Script Group*.

The following information is displayed:

Name	The user-defined script group name.
Members	The scripts that are included in the script group.
Target	The script group target.
Comments	User defined comment for the group.
Last Modified	The date and time the group was last modified.

The following options are available in the toolbar, or right-click menu.

Create New	Create a new script group.
Edit	Edit the selected group.
Delete	Delete the selected group or groups.

Run Script	Run the selected script group. If the target is <i>Device Database</i> or <i>Remote FortiGate Directly (via CLI)</i> , select the device or devices to run the scripts in the group on, then click <i>Run Now</i> . If the target is <i>Policy Package</i> or <i>ADOM Database</i> , select the policy package from the drop-down list, then click <i>Run Now</i> .
Search	Enter a search term in the search field to search the script groups.

To create a new CLI script group:

1. Go to *Device Manager > Scripts > CLI Script Group*.
2. Select *Create New* in the toolbar. The *Create New CLI Script Group(s)* pane opens.
3. Configure the following settings, then click *OK* to create the CLI script group.:

Script Group Name	Enter a name for the script group.
Comments	Optionally, type a comment for the script group.
Type	CLI Script. This field is read-only.
Run Script on	Select the script target. This settings will affect the options presented when you go to run a script. The options include: <ul style="list-style-type: none"> • <i>Device Database</i> • <i>Policy Package or ADOM Database</i> • <i>Remote FortiGate Directly (via CLI)</i>
Members	Use the directional arrows to move available scripts to member scripts.

Script syntax

Most script syntax is the same as that used by FortiOS. For information see the *FortiOS CLI Reference*, available in the [Fortinet Document Library](#).

Some special syntax is required by the FortiManager to run CLI scripts on devices.

Syntax applicable for address and address6

```
config firewall address
edit xxxx

...regular FOS command here...

config dynamic_mapping
edit "<dev_name>"-"<vdom_name>"
set subnet x.x.x.x x.x.x.x
next
end
```

Syntax applicable for ippool and ippool6

```
config firewall ippool
edit xxxx
```

```

...regular FOS command here...

config dynamic_mapping
  edit "<dev_name>"-"<vdom_name>"
    set startip x.x.x.x
    set endip x.x.x.x
  next
end

```

Syntax applicable for vip, vip6, vip46, and vip64

```

config firewall vip
  edit xxxx

...regular FOS command here...

config dynamic_mapping
  edit "<dev_name>"-"<vdom_name>"
    set extintf "any"
    set extip x.x.x.x-x.x.x.x
    set mappedip x.x.x.x-x.x.x.x
    set arp-reply enable|disable
  next
end

```

Syntax applicable for dynamic zone

```

config dynamic interface
  edit xxxx
    set single-intf disable
    set default-mapping enable|disable
    set defmap-intf xxxx
    config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
        set local-intf xxxx
        set intrazone-deny enable|disable
      next
    end
  next
end

```

Syntax applicable for dynamic interface

```

config dynamic interface
  edit xxxx
    set single-intf enable
    set default-mapping enable|disable
    set defmap-intf xxxx
    config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
        set local-intf xxxx
        set intrazone-deny enable|disable
      next
    end
  next
end

```

```
end
```

Syntax applicable for dynamic multicast interface

```
config dynamic multicast interface
  edit xxx
    set description xxx
    config dynamic_mapping
      edit "fgtname"-"vdom"
        set local-intf xxx
      next
    end
  next
end
```

Syntax applicable for local certificate (dynamic mapping)

```
config dynamic certificate local
  edit xxxx
    config dynamic_mapping
      edit "<dev_name>"-"global"
        set local-cert xxxx
      next
    end
```

Syntax applicable for vpn tunnel

```
config dynamic vpntunnel
  edit xxxx
    config dynamic_mapping
      edit "<dev_name>"-"<vdom_name>"
        set local-ipsec "<tunnel_name>"
      next
    end
```

Syntax applicable for vpn console table

```
config vpnmgr vpntable
  edit xxxx
    set topology star|meshed|dial
    set psk-auto-generate enable|disable
    set psksecret xxxx
    set ike1proposal 3des-sha1 3des-md5 ...
    set ike1dhgroup XXXX
    set ike1keylifeseq 28800
    set ike1mode aggressive|main
    set ike1dpd enable|disable
    set ike1nat traversal enable|disable
    set ike1nat keepalive 10
    set ike2proposal 3des-sha1 3des-md5
    set ike2dhgroup 5
    set ike2keylifetype seconds|kbyte|both
    set ike2keylifeseq 1800
    set ike2keylifekbs 5120
    set ike2keepalive enable|disable
    set replay enable|disable
```

```

    set pfs enable|disable
    set ike2autonego enable|disable
    set fcc-enforcement enable|disable
    set localid-type auto|fqdn|user-fqdn|keyid|addressasn1dn
    set authmethod psk|signature
    set inter-vdom enable|disable
    set certificate XXXX
  next
end

```

Syntax applicable for vpn console node

```

config vpnmgr node
  edit "1"
    set vpntable "<table_name>"
    set role hub|spoke
    set iface xxxx
    set hub_iface xxxx
    set automatic_routing enable|disable
    set extgw_p2_per_net enable|disable
    set banner xxxx
    set route-overlap use-old|use-new|allow
    set dns-mode manual|auto
    set domain xxxx
    set local-gw x.x.x.x
    set unity-support enable|disable
    set xauthtype disable|client|pap|chap|auto
    set authusr xxxx
    set authpasswd xxxx
    set authusrgrp xxxx
    set public-ip x.x.x.x
    config protected_subnet
      edit 1
        set addr xxxx xxxx ...
      next
    end
  end

```

Syntax applicable for setting installation target on policy package

```

config firewall policy
  edit x

    ...regular policy command here...

    set _scope "<dev_name>"-"<vdom_name>"
  next
end

```

Syntax applicable for global policy

```

config global header policy

  ...regular policy command here...

end

```

```
config global footer policy

...regular policy command here...

end
```

Script history

The execution history of scripts run on specific devices can be viewed from a device's dashboard. The script log can be viewed in the Task Monitor. The script execution history table also allows for viewing the script history, and re-running the script.

To view the script execution history:

1. Go to *Device Manager > Device & Groups*.
2. In the tree menu, select the device group, for example, *Managed FortiGates*. The list of devices display in the content pane and in the bottom tree menu.
3. In the bottom tree menu, select the device whose script history you want to view. The *System: Dashboard* for the device displays in the content pane.
4. In the *Configuration and Installation Status* widget, select *View History* in the *Script Status* field to open the *Script Execution History* pane.
5. To view the script history for a specific script, select the *Browse* icon in the far right column of the table to open the *Script History* dialog box.
6. To re-run a script, select the *Run script now* icon in the far right column of the table. The script is re-run. See [Run a script on page 161](#).
7. Select *Return* to return to the device dashboard.

To view a script log:

1. Go to *System Settings > Task Monitor*.
 2. Locate the script execution task whose log you need to view, and expand the task.
 3. Select the *History* icon to open the script log window.
- For more information, see [Task Monitor on page 508](#).

Script samples

This section helps familiarize you with FortiManager scripts, provides some script samples, and provides some troubleshooting tips.

The scripts presented in this section are in an easy to read format that includes:

- the purpose or title of the script
- the script itself
- the output from the script (blank lines are removed from some output)
- any variations that may be useful
- which versions of FortiOS this script will execute on



Do not include `\r` in your scripts as this will cause the script to not process properly.

Script samples includes:

- [CLI scripts](#)
- [Tcl scripts](#)

CLI scripts

CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device. CLI scripts do not include Tool Command Language (Tcl) commands, and the first line of the script is not “#!” as it is for Tcl scripts.

CLI scripts are useful for specific tasks such as configuring a routing table, adding new firewall policies, or getting system information. These example tasks easily apply to any or all FortiGate devices connected to the FortiManager system.

However, the more complex a CLI script becomes the less it can be used with all FortiGate devices - it quickly becomes tied to one particular device or configuration. One example of this is any script that includes the specific IP address of a FortiGate device's interfaces cannot be executed on a different FortiGate device.

Samples of CLI scripts have been included to help get you started writing your own scripts for your network administration tasks.

Error messages will help you determine the causes of any CLI scripting problems, and fix them. For more information, see [Error Messages on page 177](#).

The troubleshooting tips section provides some suggestions on how to quickly locate and fix problems in your CLI scripts. For more information, see [Troubleshooting Tips on page 177](#).

CLI script samples

There are two types of CLI scripts. The first type is getting information from your FortiGate device. The second type is changing information on your FortiGate device.

Getting information remotely is one of the main purposes of your FortiManager system, and CLI scripts allow you to access any information on your FortiGate devices. Getting information typically involves only one line of script as the following scripts show.

To view interface information for port1:

Script	<code>show system interface port1</code>
---------------	--

Output

```

config system interface
  edit "port1"
    set vdom "root"
    set ip 172.20.120.148 255.255.255.0
    set allowaccess ping https ssh
    set type physical
  next
end

```

Variations

Remove the interface name to see a list that includes all the interfaces on the FortiGate device including virtual interfaces such as VLANs.

Note

This script does not work when run on a policy package.

If the preceding script is used to be run on the FortiGate Directly (via CLI) or run on device database on a FortiGate has the VDOM enabled. The script will have be modified to the following:

```

config global
  show system interface port1
end

```

Since running on device database does not yield any useful information.

View the log of script running on device: FortiGate-VM64-70

```

----- Executing time: 2013-10-15 13:27:32 -----
Starting log (Run on database)
config global
end
Running script on DB success
----- The end of log -----

```

The script should be run on the FortiGate Directly (via CLI).

View the log of script running on device: FortiGate-VM64-70

```

----- Executing time: 2013-10-15 13:52:02 -----
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ show system interface port1
config system interface
  edit "port1"
    set vdom "root"
    set ip 10.2.66.181 255.255.0.0
    set allowaccess ping https ssh snmp http telnet fgfm auto-ipsec
      radius-acct probe-response capwap
    set type physical
    set snmp-index 1
  next
end
FortiGate-VM64 (global) $ end
----- The end of log -----

```

To view the entries in the static routing table. To get any useful information, the script has to be re-written for the following if the VDOM is enabled for FortiGate and has to be run on the FortiGate Directly (via CLI).

```
config vdom
  edit root
    show route static
  next
end
```

Here is a sample run of the preceding script running on the FortiGate Directly (via CLI).

View the log of script running on device: FortiGate-VM64-70

```
----- Executing time: 2013-10-15 14:24:10 -----
Starting log (Run on device)
FortiGate-VM64 $ config vdom
FortiGate-VM64 (vdom) $ edit root
current vf=root:0
FortiGate-VM64 (root) $ show route static
config router static
  edit 1
    set device "port1"
    set gateway 10.2.0.250
  next
end
FortiGate-VM64 (root) $ next
FortiGate-VM64 (vdom) $ end
----- The end of log -----
```

To view the entries in the static routing table:

Script	show route static
Output	<pre>config router static edit 1 set device "port1" set gateway 172.20.120.2 next edit 2 set device "port2" set distance 7 set dst 172.20.120.0 255.255.255.0 set gateway 172.20.120.2 next end</pre>
Variations	none

View information about all the configured FDN servers on this device:

Script	<pre>config global diag debug rating end</pre>
---------------	--

Output

View the log of script running on device: FortiGate-VM64

```
----- Executing time: 2013-10-15 14:32:15 -----
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ diagnose debug rating
Locale : english
License : Contract
Expiration : Thu Jan 3 17:00:00 2030
-- Server List (Tue Oct 15 14:32:49 2013) --
IP Weight RTT Flags TZ Packets Curr Lost Total Lost
192.168.100.206 35 2 DIF -8 4068 72 305
192.168.100.188 36 2 F -8 4052 72 308
FortiGate-VM64 (global) $ end
----- The end of log -----
```

Variations

Output for this script will vary based on the state of the FortiGate device. The preceding output is for a FortiGate device that has never been registered.

For a registered FortiGate device without a valid license, the output would be similar to:

```
Locale : english
License : Unknown
Expiration : N/A
Hostname : guard.fortinet.net

-- Server List (Tue Oct 3 09:34:46 2006) --

IP Weight Round-time TZ Packets Curr Lost Total Lost
** None **
```

Setting FortiGate device information with CLI scripts gives you access to more settings and allows you more fine grained control than you may have in the *Device Manager*. Also CLI commands allow access to more advanced options that are not available in the FortiGate GUI. Scripts that set information require more lines.



Any scripts that you will be running on the global database must include the full CLI commands and not use short forms for the commands. Short form commands will not run on the global database.

Create a new account profile called `policy_admin` allowing read-only access to policy related areas:
Script

```
config global
  config system accprofile
    edit "policy_admin"
      set fwgrp read
      set loggrp read
      set sysgrp read
    next
  end
end
```

Output

View the log of script running on device:FortiGate-VM64

```

----- Executing time: 2013-10-16 13:39:35 -----
Starting log (Run on device)
FortiGate-VM64 $ config global
FortiGate-VM64 (global) $ config system accprofile
FortiGate-VM64 (accprofile) $ edit "prof_admin"
FortiGate-VM64 (prof_admin) $ set fwgrp read
FortiGate-VM64 (prof_admin) $ set loggrp read
FortiGate-VM64 (prof_admin) $ set sysgrp read
FortiGate-VM64 (prof_admin) $ next
FortiGate-VM64 (accprofile) $ end
FortiGate-VM64 (global) $ end
----- The end of log -----

```

Variations

This profile is read-only to allow a policy administrator to monitor this device's configuration and traffic.

Variations may include enabling other areas as read-only or write permissions based on that account type's needs.

With the introduction of global objects/security console (global database), you can run a CLI script on the FortiManager global database in addition to running it on a FortiGate unit directly. Compare the following sample scripts:

- Running a CLI script on a FortiGate unit

```

config vdom
  edit "root"
    config firewall policy
      edit 10
        set srcintf "port5"
        set dstintf "port6"
        set srcaddr "all"
        set dstaddr "all"
        set status disable
        set schedule "always"
        set service "ALL"
        set logtraffic disable
      next
    end
  end

```

- Running a CLI script on the global database

```

config firewall policy
  edit 10
    set srcintf "port5"
    set dstintf "port6"
    set srcaddr "all"
    set dstaddr "all"
    set status disable
    set schedule "always"
    set service "ALL"
    set logtraffic disable
  next
end

```

Error Messages

Most error messages you will see are regular FortiGate CLI error messages. If you are familiar with the CLI you will likely recognize them.

Other error messages indicate your script encountered problems while executing, such as:

- `command parse error`: It was not possible to parse this line of your script into a valid FortiGate CLI command. Common causes for this are misspelled keywords or an incorrect command format.
- `unknown action`: Generally this message indicates the previous line of the script was not executed, especially if the previous line accesses an object such as “config router static”.
- `Device XXX failed-1`: This usually means there is a problem with the end of the script. XXX is the name of the FortiGate unit the script is to be executed on. If a script has no end statement or that line has an error in it you may see this error message. You may also see this message if the FortiGate unit has not been synchronized by deploying its current configuration.

Troubleshooting Tips

Here are some troubleshooting tips to help locate and fix problems you may experience with your scripts.

- Check the script output. Generally the error messages displayed here will help you locate and fix the problem.
- See the *FortiGate CLI Reference* for more information on all CLI commands.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.
- As mentioned at the start of this chapter, ensure the `console more` command is disabled on the FortiGate devices where scripts execute. Otherwise a condition may occur where both the FortiGate device and the FortiManager system are waiting for each other to respond until they timeout.
- There should be no punctuation at the start or end of the lines.
- Only whitespace is allowed on the same line as the command. This is useful in lining up `end` and `next` commands for quick and easy debugging of the script.
- Keep your scripts short. They are easier to troubleshoot and it gives you more flexibility. You can easily execute a number of scripts after each other.
- Use full command names. For example instead of “set host test” use “set hostname test”. This is required for any scripts that are to be run on the global database.
- Use the number sign (#) to comment out a line you suspect contains an error.

Tcl scripts

Tcl is a dynamic scripting language that extends the functionality of CLI scripting. In FortiManager Tcl scripts, the first line of the script is “#!” as it is for standard Tcl scripts.



Do not include the exit command that normally ends Tcl scripts; it will prevent the script from running.

This guide assumes you are familiar with the Tcl language and regular expressions, and instead focuses on how to use CLI commands in your Tcl scripts. Where you require more information about Tcl commands than this guide contains,

please refer to resources such as the Tcl newsgroup, Tcl reference books, and the official Tcl website at <http://www.tcl.tk>.

Tcl scripts can do more than just get and set information. The benefits of Tcl come from:

- variables to store information,
- loops to repeats commands that are slightly different each time
- decisions to compare information from the device

The sample scripts in this section will contain procedures that you can combine to use your scripts. The samples will each focus on one of four areas:

- [Tcl variables](#)
- [Tcl loops](#)
- [Tcl decisions](#)
- [Tcl file IO](#)

To enable Tcl scripting, use the following CLI commands:

```
config system admin setting
    set show_tcl_script enable
end
```

Limitations of FortiManager Tcl

FortiManager Tcl executes in a controlled environment. You do not have to know the location of the Tcl interpreter or environment variables to execute your scripts. This also means some of the commands normally found in Tcl are not used in FortiManager Tcl.

Depending on the CLI commands you use in your Tcl scripts, you may not be able to run some scripts on some versions of FortiOS as CLI commands change periodically.



Before testing a new script on a FortiGate device, you should backup that device's configuration and data to ensure it is not lost if the script does not work as expected.

Tcl variables

Variables allow you to store information from the FortiGate device, and use it later in the script. Arrays allow you to easily manage information by storing multiple pieces of data under a variable name. The next script uses an array to store the FortiGate system information.

Example: Save system status information in an array.

Script:

```
#!/
proc get_sys_status aname {
    upvar $aname a
    puts [exec "# This is an example Tcl script to get the system status of the FortiGate\n" "# "
        15 ]
    set input [exec "get system status\n" "# " 15 ]
    # puts $input
```

```

    set linelist [split $input \n]
# puts $linelist
foreach line $linelist {
    if {[regexp {[^:]+:(.*)} $line dummy key value]} continue
    switch -regexp -- $key {
        Version {
            regexp {FortiGate-([^\s]+) ([^\s,]+),build([\d]+),.*} $value dummy a(platform) a(version) a
                (build)
        }
        Serial-Number {
            set a(serial-number) [string trim $value]
        }
        Hostname {
            set a(hostname) [string trim $value]
        }
    }
}
get_sys_status status
puts "This machine is a $status(platform) platform."
puts "It is running version $status(version) of FortiOS."
puts "The firmware is build# $status(build)."
puts "S/N: $status(serial-number)"
puts "This machine is called $status(hostname)"

```

Output:

```

----- Executing time: 2013-10-21 09:58:06 -----
Starting log (Run on device)

FortiGate-VM64 #

This machine is a VM64 platform.
It is running version v5.0 of FortiOS.
The firmware is build# 0228.
S/N: FGVM02Q105060070
This machine is called FortiGate-VM64

----- The end of log -----

```

Variations:

Once the information is in the variable array, you can use it as part of commands you send to the FortiGate device or to make decisions based on the information. For example:

```

if {$status(version) == 5.0} {
# follow the version 5.0 commands
} elseif {$status(version) == 5.0} {
# follow the version 5.0 commands
}

```

This script introduces the concept of executing CLI commands within Tcl scripts using the following method:

```
set input [exec "get system status\n" "# "]
```

This command executes the CLI command “get system status” and passes the result into the variable called input. Without the “\n” at the end of the CLI command, the CLI command will not execute to provide output.

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- lines 2-3 open the procedure declaration

- lines 4-5 puts the output from the CLI command into a Tcl variable as a string, and breaks it up at each return character into an array of smaller strings
- line 6 starts a loop to go through the array of strings
- line 7 loops if the array element is punctuation or continues if its text
- line 8 takes the output of line 7's regular expression command and based on a match, performs one of the actions listed in lines 9 through 17
- lines 9-11 if regular expression matches 'Version' then parse the text and store values for the platform, version, and build number in the named array elements
- line 12-14 if regular expression matches 'Serial-Number' then store the value in an array element named that after trimming the string down to text only
- lines 15-17 is similar to line 12 except the regular expression is matched against 'Hostname'
- line 17-19 close the switch decision statement, the for each loop, and the procedure
- line 20 calls the procedure with an array name of status
- lines 21-25 output the information stored in the status array

Tcl loops

Even though the last script used a loop, that script's main purpose was storing information in the array. The next script uses a loop to create a preset number of users on the FortiGate device, in this case 10 users. The output is only shown for the first two users due to space considerations.

Example: Create 10 users from usr0001 to usr0010:

Script:

```
#!/
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# " 15]
}
  set num_users 10
do_cmd "config vdom"
do_cmd "edit root"
do_cmd "config user local"
for {set i 1} {$i <= $num_users} {incr i} {
  set name [format "usr%04d" $i]
  puts "Adding user: $name"
  do_cmd "edit $name"
  do_cmd "set status enable"
  do_cmd "set type password"
  do_cmd "next"
}
do_cmd "end"
do_cmd "end"

do_cmd "config vdom"
do_cmd "edit root"
do_cmd "show user local"
do_cmd "end"
```

Output:

View the log of script running on device:FortiGate-VM64

```
----- Executing time: 2013-10-16 15:27:18 -----
```



```
Starting log (Run on device)
config vdom
FortiGate-VM64 (vdom) #
edit root
current vf=root:0
FortiGate-VM64 (root) #
config user local
FortiGate-VM64 (local) #
Adding user: usr0001
edit usr0001
new entry 'usr0001' added
FortiGate-VM64 (usr0001) #
set status enable
FortiGate-VM64 (usr0001) #
set type password
FortiGate-VM64 (usr0001) #
next
```

```
FortiGate-VM64 (local) #
Adding user: usr0002
edit usr0002
new entry 'usr0002' added
FortiGate-VM64 (usr0002) #
set status enable
FortiGate-VM64 (usr0002) #
set type password
FortiGate-VM64 (usr0002) #
next
```

Variations:

There are a number of uses for this kind of looping script. One example is to create firewall policies for each interface that deny all non-HTTPS and non-SSH traffic by default. Another example is a scheduled script to loop through the static routing table to check that each entry is still reachable, and if not remove it from the table.

This script loops 10 times creating a new user each time whose name is based on the loop counter. The format command is used to force a four digit number.

In analyzing this script:

- line 1 is the required `#!` to indicate this is a Tcl script
- lines 2-4 open CLI command wrapper procedure
- line 5 declares the number of users to create
- line 6 gets the FortiGate ready for entering local users
- line 7 opens the for loop that will loop ten times
- line 8 sets the user name based on the incremented loop counter variable
- line 9 is just a comment to the administrator which user is being created
- lines 10-13 create and configure the user, leaving the CLI ready for the next user to be added
- line 14 ends the for loop
- line 15 ends the adding of users in the CLI
- line 16 executes a CLI command to prove the users were added properly

Tcl decisions

Tcl has a number of decision structures that allow you to execute different CLI commands based on what information you discover.

This script is more complex than the previous scripts as it uses two procedures that read FortiGate information, make a decision based on that information, and then executes one of the CLI sub-scripts based on that information.

Example: Add information to existing firewall policies.

Script:

```
#!/
# need to define procedure do_cmd
# the second parameter of exec should be "# "
# If split one command to multiple lines use "\" to continue
proc do_cmd {cmd} {
    puts [exec "$cmd\n" "# "]
}
foreach line [split [exec "show firewall policy\n" "# "] \n] {
    if {[regexp {edit[ ]+([0-9]+)} $line match policyid]} {
        continue
    } elseif {[regexp {set[ ]+(\w+)[ ]+(.*)\r} $line match key value]} {
        lappend fw_policy($policyid) "$key $value"
    }
}
do_cmd "config firewall policy"
foreach policyid [array names fw_policy] {
    if {[lsearch $fw_policy($policyid){diffservcode_forward 000011}] == -1} {
        do_cmd "edit $policyid"
        do_cmd "set diffserv-forward enable"
        do_cmd "set diffservcode-forward 000011"
        do_cmd "next"
    }
}
do_cmd "end"
```

Variations:

This type of script is useful for updating long lists of records. For example if the FortiOS version adds new keywords to user accounts, you can create a script similar to this one to get the list of user accounts and for each one edit it, add the new information, and move on to the next.

This script uses two decision statements. Both are involved in text matching. The first decision is checking each line of input for the policy ID and if its not there it skips the line. If it is there, all the policy information is saved to an array for future use. The second decision searches the array of policy information to see which polices are miss

In analyzing this script:

- line 1 is the required #! to indicate this is a Tcl script
- line 2-8 is a loop that reads each policy's information and appends only the policy ID number to an array variable called fw_policy
- line 9 opens the CLI to the firewall policy section to prepare for the loop
- line 10 starts the for each loop that increments through all the firewall policy names stored in fw_policy
- line 11 checks each policy for an existing diffservcode_forward 000011 entry - if its not found lines 12-15 are executed, otherwise they are skipped

- line 12 opens the policy determined by the loop counter
- line 13-14 enable `diffserv_forward`, and set it to 000011
- line 15 saves this entry and prepares for the next one
- line 16 closes the if statement
- line 17 closes the for each loop
- line 18 saves all the updated firewall policy entries

Additional Tcl Scripts

Example: Get and display state information about the FortiGate device:

Script:

```
#!/
#Run on FortiOS v5.00
#This script will display FortiGate's CPU states,
#Memory states, and Up time
puts [exec "# This is an example Tcl script to get the system performance of the FortiGate\n"
      "# " 15 ]
      set input [exec "get system status\n" "# " 15]
      regexp {Version: *([^\ ]+) ([^\,]+),build([0-9]+),[0-9]+} $input dummy status(Platform) status
        (Version) status(Build)
      if {$status(Version) eq "v5.0"} {
        puts -nonewline [exec "config global\n" "# " 30]
        puts -nonewline [exec "get system performance status\n" "# " 30]
        puts -nonewline [exec "end\n" "# " 30]
      } else {
        puts -nonewline [exec "get system performance\n" "# " 30]
      }
}
```

Output:

```
----- Executing time: 2013-10-21 16:21:43 -----
Starting log (Run on device)

FortiGate-VM64 #
config global
FortiGate-VM64 (global) # get system performance status

CPU states: 0% user 0% system 0% nice 90% idle
CPU0 states: 0% user 0% system 0% nice 90% idle
CPU1 states: 0% user 0% system 0% nice 90% idle
Memory states: 73% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 0 kbps in 30 minutes
Average sessions: 1 sessions in 1 minute, 2 sessions in 10 minutes, 2 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in
      last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 6 days, 1 hours, 34 minutes

FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----

----- Executing time: 2013-10-21 16:16:58 -----
```

Example: Configure common global settings.**Script:**

```
#!/
#Run on FortiOS v5.00
#This script will configure common global, user group and ntp settings
#if you do not want to set a parameter, comment the
#corresponding set command
#if you want to reset a parameter to it's default
#value, set it an empty string
puts [exec "# This is an example Tcl script to configure global, user group and ntp setting of
FortiGate\n" "# " 15 ]

# global
set sys_global(admintimeout) ""
# user group
set sys_user_group(authtimeout) 20
# ntp
set sys_ntp(source-ip) "0.0.0.0"
set sys_ntp(ntpsync) "enable"
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# " 30]
}
#config system global---begin
fgt_cmd "config global"
fgt_cmd "config system global"
foreach key [array names sys_global] {
if {$sys_global($key) ne ""} {
fgt_cmd "set $key $sys_global($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system global---end

#config system user group---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config user group"
fgt_cmd "edit groupname"
foreach key [array names sys_user_group] {
if {$sys_user_group($key) ne ""} {
fgt_cmd "set $key $sys_user_group($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system user group---end

#config system ntp---begin
fgt_cmd "config global"
fgt_cmd "config system ntp"
```

```
foreach key [array names sys_ntp] {
if {$sys_ntp($key) ne ""} {
fgt_cmd "set $key $sys_ntp($key)"
} else {
fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system ntp---end
```

Output:

```
----- Executing time: 2013-10-22 09:12:57 -----
Starting log (Run on device)

FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # unset admintimeout
FortiGate-VM64 (global) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config user group
FortiGate-VM64 (group) # edit groupname
FortiGate-VM64 (groupname) # set authtimeout 20
FortiGate-VM64 (groupname) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system ntp
FortiGate-VM64 (ntp) # set ntpsync enable
FortiGate-VM64 (ntp) # set source-ip 0.0.0.0
FortiGate-VM64 (ntp) # end
FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----
```

Example: Configure syslogd settings and filters.

Script:

```
#!
#Run on FortiOS v5.00
#This script will configure log syslogd setting and
#filter
#key-value pairs for 'config log syslogd setting', no
#value means default value.
    set setting_list {{status enable} {csv enable}
{facility alert} {port} {server 1.1.1.2}}
#key-value pairs for 'config log syslogd filter', no
#value means default value.
puts [exec "# This is an example Tcl script to configure log syslogd setting and filter
    setting of FortiGate\n" "# " 15 ]
    set filter_list {{attack enable} {email enable} {severity} {traffic enable} {virus disable}
{web enable}}
#set the number of syslogd server, "", "2" or "3"
    set syslogd_no "2"
```

```
#procedure to execute FortiGate CLI command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
    set len [llength $kv]
    if {$len == 0} {
        continue
    } elseif {$len == 1} {
        fgt_cmd "unset [lindex $kv 0]"
    } else {
        fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
    } } }
#configure log syslogd setting---begin
fgt_cmd "config global"
fgt_cmd "config log syslogd$syslogd_no setting"
    set_kv $setting_list
fgt_cmd "end"
#configure log syslogd setting---end
#configure log syslogd filter---begin
fgt_cmd "config log syslogd$syslogd_no filter"
    set_kv $filter_list
fgt_cmd "end"
#configure log syslogd filter---end
```

Output:

Starting log (Run on device)

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config log syslogd2 setting
FortiGate-VM64 (setting) # set status enable
FortiGate-VM64 (setting) # set csv enable
FortiGate-VM64 (setting) # set facility alert
FortiGate-VM64 (setting) # unset port
FortiGate-VM64 (setting) # set server 1.1.1.2
FortiGate-VM64 (setting) # end
```

```
FortiGate-VM64 (global) # config log syslogd2 filter
FortiGate-VM64 (filter) # set attack enable
FortiGate-VM64 (filter) # set email enable
FortiGate-VM64 (filter) # unset severity
FortiGate-VM64 (filter) # set traffic enable
FortiGate-VM64 (filter) # set virus disable
FortiGate-VM64 (filter) # set web enable
FortiGate-VM64 (filter) # end
FortiGate-VM64 (global) #
```

----- The end of log -----

Example: Configure the FortiGate device to communicate with a FortiAnalyzer unit:

Script:

```
#!
#This script will configure the FortiGate device to
```

```

#communicate with a FortiAnalyzer unit
#Enter the following key-value pairs for 'config
#system fortianalyzer'
    set status enable
    set enc-algorithm high
#localid will be set as the hostname automatically
#later
puts [exec "# This is an example Tcl script to configure the FortiGate to communicate with a
    FortiAnalyzer\n" "# " 15 ]
    set server 1.1.1.1
#for fortianalyzer, fortianalyzer2 or
#fortianalyzer3, enter the corresponding value "",
#"2", "3"
    set faz_no ""
#keys used for 'config system fortianalyzer', if you
#do not want to change the value of a key, do not put
#it in the list
    set key_list {status enc-algorithm localid server }
##procedure to get system status from a FortiGate
proc get_sys_status aname {
upvar $aname a
set input [split [exec "get system status\n" "# " ] \n]
foreach line $input {
if {[regexp {[^:]+}:(.*)} $line dummy key value]} continue
    set a([string trim $key]) [string trim $value]
}
}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#set the localid as the FortiGate's hostname
get_sys_status sys_status
set localid $sys_status(Hostname)
#config system fortianalyzer---begin
fgt_cmd "config global"
fgt_cmd "config log fortianalyzer$faz_no setting"
foreach key $key_list {
if [info exists $key] {
    fgt_cmd "set $key [set $key]"
} else {
    fgt_cmd "unset $key"
}
}
fgt_cmd "end"
fgt_cmd "end"
#config system fortianalyzer---end

```

Output:

```

Starting log (Run on device)
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config log fortianalyzer setting
FortiGate-VM64 (setting) # set status enable
FortiGate-VM64 (setting) # set enc-algorithm high
FortiGate-VM64 (setting) # set localid FortiGate-VM64
FortiGate-VM64 (setting) # set server 1.1.1.1
FortiGate-VM64 (setting) # end

```

```
FortiGate-VM64 (global) # end
FortiGate-VM64 #
----- The end of log -----
```

Example: Create custom IPS signatures and add them to a custom group.

Script:

```
#!/
#Run on FortiOS v5.00
#This script will create custom ips signatures and
#change the settings for the custom ips signatures

puts [exec "# This is an example Tcl script to create custom ips signatures and change the
settings for the custom ips signatures on a FortiGate\n" "# " 15 ]
#Enter custom ips signatures, signature names are the
#names of array elements
set custom_sig(c1) {"F-SBID(--protocol icmp;--icmp_type 10; )"}
set custom_sig(c2) {"F-SBID(--protocol icmp;--icmp_type 0; )"}
#Enter custom ips settings
set custom_rule(c1) {{status enable} {action block} {log enable} {log-packet} {severity
high}}
set custom_rule(c2) {{status enable} {action pass} {log} {log-packet disable} {severity
low}}
#procedure to execute FortiGate command
proc fgt_cmd cmd {
puts -nonewline [exec "$cmd\n" "# "]
}
#procedure to set a series of key-value pairs
proc set_kv kv_list {
foreach kv $kv_list {
set len [llength $kv]
if {$len == 0} {
continue
} elseif {$len == 1} {
fgt_cmd "unset [lindex $kv 0]"
} else {
fgt_cmd "set [lindex $kv 0] [lindex $kv 1]"
}
}
}
#config ips custom---begin
fgt_cmd "config vdom"
fgt_cmd "edit root"
fgt_cmd "config ips custom"
foreach sig_name [array names custom_sig] {
fgt_cmd "edit $sig_name"
fgt_cmd "set signature $custom_sig($sig_name)"
fgt_cmd "next"
}
fgt_cmd "end"
#config ips custom settings---begin
foreach rule_name [array names custom_rule] {
fgt_cmd "config ips custom"
fgt_cmd "edit $rule_name"
set_kv $custom_rule($rule_name)
fgt_cmd "end"
}
fgt_cmd "end"
```



```
#config ips custom settings---end
```

Output:

```
Starting log (Run on device)
FortiGate-VM64 # config vdom
FortiGate-VM64 (vdom) # edit root
current vf=root:0
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # set signature "F-SBID(--protocol icmp;--icmp_type 10; )"
FortiGate-VM64 (c1) # next
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set signature "F-SBID(--protocol icmp;--icmp_type 0; )"
FortiGate-VM64 (c2) # next
FortiGate-VM64 (custom) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c1
FortiGate-VM64 (c1) # set status enable
FortiGate-VM64 (c1) # set action block
FortiGate-VM64 (c1) # set log enable
FortiGate-VM64 (c1) # unset log-packet
FortiGate-VM64 (c1) # set severity high
FortiGate-VM64 (c1) # end
FortiGate-VM64 (root) # config ips custom
FortiGate-VM64 (custom) # edit c2
FortiGate-VM64 (c2) # set status enable
FortiGate-VM64 (c2) # set action pass
FortiGate-VM64 (c2) # unset log
FortiGate-VM64 (c2) # set log-packet disable
FortiGate-VM64 (c2) # set severity low
FortiGate-VM64 (c2) # end
FortiGate-VM64 (root) # end
FortiGate-VM64 #
----- The end of log -----
```

Variations:

None.

Tcl file IO

You can write to and read from files using Tcl scripts. For security reasons there is only one directory on the FortiManager where scripts can access files. For this reason, there is no reason to include the directory in the file name you are accessing. For example “/var/temp/myfile” or “~/myfile” will cause an error, but “myfile” or “/myfile” is OK.

The Tcl commands that are supported for file IO are: file, open, gets, read, tell, seek, eof, flush, close, fcopy, fconfigure, and fileevent.

The Tcl file command only supports delete subcommand, and does not support the -force option.

There is 10MB of disk space allocated for Tcl scripts. An error will be reported if this size is exceeded.

These files will be reset when the following CLI commands are run: `exec format`, `exec reset partition`, or `exec reset all`. The files will not be reset when the firmware is updated unless otherwise specified.

To write to a file:

```
Script      #!/
set somefile [open "tcl_test" w]
puts $somefile "Hello, world!"
close $somefile
```

To read from a file:

```
Script      #!/
set otherfile [open "tcl_test" r]
while {[gets $otherfile line] >= 0} {
puts [string length $line]
}
close $otherfile
```

```
Output      Hello, world!
```

These two short scripts write a file called `tcl_test` and then read it back.

Line 3 in both scripts opens the file either for reading (r) or writing (w) and assigns it to a filehandle (somefile or otherfile). Later in the script when you see these filehandles, its input or output passing to the open file.

When reading from the file, lines 4 and 5 loop through the file line by line until it reaches the end of the file. Each line that is read is put to the screen.

Both scripts close the file before they exit.

Troubleshooting Tips

This section includes suggestions to help you find and fix problems you may be having with your scripts.

- Make sure the commands you are trying to execute are valid for the version of FortiOS running on your target FortiGate device.
- You should always use braces when evaluating code that may contain user input, to avoid possible security breaches. To illustrate the danger, consider this interactive session:

```
% set userinput {[puts DANGER!]}
[puts DANGER!]
% expr $userinput == 1
DANGER!
0
% expr {$userinput == 1}
0
```

In the first example, the code contained in the user-supplied input is evaluated, whereas in the second the braces prevent this potential danger. As a general rule, always surround expressions with braces, whether using `expr` directly or some other command that takes an expression.

- A number that includes a leading zero or zeros, such as 0500 or 0011, is interpreted as an octal number, not a decimal number. So 0500 is actually 320 in decimal, and 0011 is 9 in decimal.
- There is a limit to the number of scripts allowed on the FortiManager unit. Try removing an old script before trying to save your current one.

- Using the Tcl command “catch” you can add custom error messages in your script to alert you to problems during the script execution. When catch encounters an error it will return 1, but if there is no error it will return 0. For example:

```
if { [catch {open $someFile w} fid] } {
    puts stderr "Could not open $someFile for writing\n$fid"
    exit 1 ;# error opening the file!
} else {
    # put the rest of your script here
}
```

Use Tcl script to access FortiManager's device database or ADOM database

You can use Tcl script to access FortiManager's device database or ADOM database (local database).

Example 1:

Run the Tcl script on an ADOM database for a specify policy package. For example, creating new a policy or object:

Syntax	<code>puts [exec_ondb "/adom/<adom_name>/pkg/<pkg_fullpath>" "embedded cli commands" "# "]</code>
Usage	<code>puts [exec_ondb "/adom/52/pkg/default" " config firewall address edit port5_address next end " "# "]</code>

Example 2:

Run the Tcl script on the current ADOM database for a specify policy package. For example, creating a new policy and object:

Syntax	<code>puts [exec_ondb "/adom/./pkg/<pkg_fullpath>" "embedded cli commands" "# "] or puts [exec_ondb "/pkg/<pkg_fullpath>" "embedded cli commands" "# "]</code>
Usage	<code>puts [exec_ondb "/adom/./pkg/default" " config firewall address edit port5_address next end " "# "]</code>

Example 3:

Run Tcl script on a specific device in an ADOM:

Syntax	<code>puts [exec_ondb "/adom/<adom_name>/device/<dev_name>" "embedded cli commands" "# "]</code>
---------------	--

Usage	<pre>puts [exec_ondb "/adom/v52/device/FGT60CA" " config global config system global set admintimeout 440 end end " "# "]</pre>
--------------	---

Example 4:

Run Tcl script on current devices in an ADOM:

Syntax	<pre>puts [exec_ondb "/adom/<adom_name>/device/." "embedded cli commands" "# "]</pre>
Usage	<pre>puts [exec_ondb "/adom/v52/device/." " config global config system global set admintimeout 440 end end " "# "]</pre>



`exec_ondb` cannot be run on the Global ADOM.

SD-WAN Load Balance

When central monitoring is enabled, you can use the *Device Manager > SD-WAN > SD-WAN Status Check Profiles* pane to monitor load-balancing profiles of WAN links. When central monitoring is disabled, you must monitor load-balancing profiles by monitoring each device.

Enabling central SD-WAN

Central SD-WAN management can be enabled per ADOM. When enabled, the SD-WAN tab shows the following options in the tree menu:

- SD-WAN
- SD-WAN Status Check Profiles

To enable central SD-WAN:

1. Go to *System Settings > All ADOMs*.
2. Select the ADOM and click *Edit* in the toolbar, or right-click the ADOM and select *Edit* from the pop-up menu. The *Edit ADOM* window opens ([Editing an ADOM on page 60](#)).

3. Next to *Central Management*, select the *SD-WAN* checkbox.
4. Click *OK*.

Manage SD-WAN load balancing profiles

You can manage load balancing profiles from the *Device Manager > SD-WAN > SD-WAN* pane. Some options are located in the toolbar, and some options are available when you right-click a profile in the content pane.

Option	Description
Create New	Create a new load-balancing profile (Creating SD-WAN load balancing profiles on page 193).
Delete	Delete the selected profile.
Edit	Edit the selected profile.

Creating SD-WAN load balancing profiles

You can create a load balancing profile for WAN links of a device.

To create an SD-WAN load balancing profile:

1. Ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN* and click *Create New*. The *New SD-WAN* pane opens.
3. Configure the following options, then click *OK* to add the WAN link:

Device	Select a FortiGate device with WAN links.
Name	Displays the name of the profile.
Type	Displays the type of profile.
Administrative Status	Enable or disable the profile. Select <i>Up</i> to enable the profile, or <i>Down</i> to disable the profile.
Load Balancing Algorithm	Select a load-balancing algorithm: <ul style="list-style-type: none"> • Volume • Sessions • Spillover • Source-Destination IP • Source IP
Interface Members	Specify the interface members for which you want to balance loads. The interface members are derived from the FortiGate device. Click <i>Create New</i> to add interfaces. Select the interface, gateway IP, and status of the interface member, then click <i>OK</i> to add the interface member. Interface members can also be edited and delete from the list.

Services

Specify the priority rules for load balancing. The priority rules are derived from the FortiGate device.

Click *Create New* to add a priority rule. Enter the name of the service, then select the source address and user groups, destination address and protocol number, outgoing interface, and health check, then click *OK* to add the rule.

Rules can also be edited and deleted from the list.

Manage profiles for checking WAN link status

When central monitoring of SD-WAN load balancing is enabled, you can manage monitoring profiles from the *Device Manager > SD-WAN > SD-WAN Status Check Profile* pane. Some options are located in the toolbar, and some options are available when you right-click a profile.

Option	Description
Create New	Create a new profile for checking WAN link status.
Delete	Delete the selected profile.
Edit	Edit the selected profile.
Clone	Clone the selected profile.
Select All	Select all profiles in the content pane.

Creating profiles for checking WAN link status

When central monitoring of WAN link load balancing is enabled, you can create profiles that monitor the status of load-balancing profiles for WAN links.

To create a profile:

1. If necessary, ensure that you are in the correct ADOM.
2. Go to *Device Manager > SD-WAN > SD-WAN Status Check Profile*, and click *Create New*. The *New SD-WAN Status Check Profile* pane opens.
3. Configure the following options, then click *OK* to create the new status check profile:

Name	Enter a name for the profile.
Detect Server	Type the IP address for WAN interface that you want to monitor.
Detect Protocol	Select the detection method for the profile check: <ul style="list-style-type: none"> • Ping • TCP Echo • UDP Echo • HTTP • TWAMP

Link Status	Specify options for the WAN link status.
Timeout	Specify how many seconds before the link times out.
Failures before inactive	Specify the threshold that triggers a warning message, in milliseconds, or percent if the criteria is <i>Packet Loss</i> .
Restore link after	Specify the threshold that triggers an error message, in milliseconds, or percent if the criteria is <i>Packet Loss</i> .
Actions when Inactive	Specify what happens with the WAN link becomes inactive.
Update Static Route	Select to update the static route when the WAN link becomes inactive.
Cascade Interfaces	Select to cascade interfaces when the WAN link becomes inactive

FortiExtender

FortiExtender is managed centrally in the *Device Manager* pane. When a FortiGate in the ADOM has managed FortiExtender devices, they are listed in an *All FortiExtender* group.



FortiExtender can be managed by a FortiGate running FortiOS 5.2 or later.

Centrally managed

When managing FortiExtender centrally, FortiAP devices will be listed in the *AP Management* pane in the ADOM of the FortiGate managing the FortiExtender.

The following information is displayed:

Device Name	The serial number of the FortiGate device that is managing the FortiExtender.
Serial Number	The serial number of the FortiExtender.
Priority	The FortiExtender priority, either <i>Primary</i> or <i>Secondary</i> .
Model	The FortiExtender model.
Management Status	The FortiExtender management status, either <i>Authorized</i> or <i>Deauthorized</i> .
Status	The FortiExtender status, either <i>Up</i> or <i>Down</i> .
Network	The FortiExtender network status and carrier name.
Current Usage	The current data usage.

Last Month Usage	The data usage for the last month.
Version	The FortiExtender firmware version.

The right-click menu options include:

Refresh	Select a FortiExtender in the list, right-click, and select <i>Refresh</i> in the menu to refresh the information displayed.
Edit	Select a FortiExtender in the list, right-click, and select <i>Edit</i> in the menu to edit the FortiExtender modem settings, PPP authentication, general, GSM/LTE, and CDMA settings.
Upgrade	Select a FortiExtender in the list, right-click, and select <i>Upgrade</i> in the menu to upgrade the FortiExtender firmware.
Authorize	Select a FortiExtender in the list, right-click, and select <i>Authorize</i> in the menu to authorize the unit for management.
Deauthorize	Select a FortiExtender in the list, right-click, and select <i>Deauthorize</i> in the menu to deauthorize the unit for management.
Restart	Select a FortiExtender in the list, right-click, and select <i>Restart</i> in the menu to restart the unit.
Set Primary	Select a FortiExtender in the list, right-click, and select <i>Set Primary</i> in the menu to set the unit as the primary device.
Status	Select a FortiExtender in the list, right-click, and select <i>Status</i> in the menu to view status information including system status, modem status, and data usage.

To edit a FortiExtender:

1. Go to *Device Manager > FortiExtender*.
2. Right-click the FortiExtender device, and select *Edit*. The *Edit FortiExtender* page is displayed.
3. Configure the following settings, then click *OK* to save the setting:

Modem Settings	Configure the dial mode, redial limit, and quota limit.
PPP Authentication	Configure the user name, password, and authentication protocol.
General	Configure the usage cycle reset day, AT dial script, modem password, and the allow network initiated updates to modem setting.
GSM / LTE	Configure the access point name (APN), SIM PIN, and LTE multiple mode.
CDMA	Configure the NAI, AAA shared secret, HA shared secret, primary HA, secondary HA, AAA SPI, and HA SPI.

FortiMeter

FortiMeter allows you turn FortiOS-VMs and FortiWebOS-VMs on and off as needed, paying only for the volume and consumption of traffic that you use. These VMs are also sometimes called pay-as-you-go VMs.

You must meet the following requirements to use metered VMs:

- You must have a FortiMeter license.
- The FortiMeter license must be linked with the FortiManager unit by using FortiCare.

FortiOS VMs

FortiManager supports the following types of licenses for FortiMeter:

- Prepaid: FortiOS VM usage is prepaid by purchasing points.
- Postpaid: The FortiOS VM is billed monthly based on usage.

The license determines whether FortiMeter is prepaid or postpaid.

The VM deployment packages are included with firmware images on the [Customer Service & Support](#) site, and have the following format: FOS_VMxx-v5-buildXXXX-Fortinet.out. In FortiManager, the VM will be listed as a FortiOS VM.

FortiManager also supports metering for FortiOS VM HA clusters.

FortiWeb VMs

FortiManager supports FortiWeb devices as logging devices. FortiWeb VMs are billed monthly based on usage.

The VM deployment packages are included with firmware images on the [Customer Service & Support](#) site, and have the following format: FWB_OS1-v5xx-buildXXXX-FORTINET.out. In FortiManager, the VM will be listed as a FBV0X.

Overview

The following is an overview of how to use metered VMs:

1. Purchase a FortiMeter license. Contact your sales representative for more information.
2. Go to [FortiCare](https://support.fortinet.com/) (https://support.fortinet.com/) and log into your account.

You can also access FortiCare from FortiManager:

- From *System Settings > Dashboard*, in the *License Information* widget, click the *Purchase* icon in the *VM Meter Service* field.
- From *Device Manager > VM Meter*, click the *Purchase Points* icon in the toolbar.

3. Go to *Asset > Manage/View Products*, and locate the FortiMeter license.

4. Link the FortiMeter license with your FortiManager by using the *Link Device* option.

You can only link FortiManager to one metering group at a time.

5. If you are prepaying (FortiOS VMs only), purchase a point package and add it to the FortiMeter license using the *Add Licenses* option. See [Points on page 198](#).

6. Ensure that the VM is registered to the FortiManager. See [Adding devices on page 107](#).
7. Authorize the metered VMs in FortiManager. See [Authorizing metered VMs on page 198](#).



If connectivity between the VM and FortiManager is lost, FortiManager will invalidate the VM instance after fifteen days. If the VM reconnects before fifteen days have elapsed, it will automatically synchronize with the FortiManager database.

Points

Points can be purchased in packages of 1000 or 10000 from the FortiMeter product information page on FortiCare using the *Add Licenses* button.

Points are used based on the type of service and the volume of traffic sent to FortiGuard.

Type	Service Code	Points
VOLUME (1TB)	FW	4
VOLUME (1TB)	FWURL	10
VOLUME (1TB)	UTM	25

For prepaid FortiOS VMs, after the point balance has become negative, VMs can continue to be used for up to 15 days before the account is frozen or more points are purchased to restore a positive point balance.

With a negative point balance, the FortiMeter status will show the number of days until it is frozen, or *FREZ* when it is already frozen. FortiMeter will be unfrozen when a positive point balance is restored.

For FortiOS VM HA clusters, only the master or primary unit sends traffic to FortiMeter.

Authorizing metered VMs

You must authorize all metered VMs in FortiManager before you can use them.

Authorizing FortiOS VMs

FortiOS VMs must be registered before they can be authorized. See [Adding devices on page 107](#).

To authorize metered FortiOS VMs:

1. Ensure that the VM is registered to the FortiManager. See [Adding devices on page 107](#).
2. Ensure you are in the correct ADOM.
3. Go to *Device Manager > VM Meter*.
4. Select a device then click *Authorize* in the toolbar, right-click on a device then select *Authorize*, or double-click on a device. The *Authorize Device(s)* dialog box opens.

An unauthorized device can use firewall services for up to 48 hours.

5. Select the *License Type*:

Trial	Maximum of two devices can have a trial license at any one time. No traffic data are sent to FortiGuard, so no points are used. Can be used for up to 30 days.
Regular	Regular license. Points used based on the service level and volume of traffic going to FortiGuard.

6. Select the *Services*:

Firewall	Firewall only. This option cannot be deselected.
IPS	IPS services.
Web Filter	Web filtering services.
AntiVirus	Antivirus services.
App Control	Application control services.
Full UTM	All services are selected.

7. Click *OK* to authorize the device.

Authorizing FortiWeb VMs

FortiWeb VMs must be registered manually before they can be authorized. See [Adding devices manually on page 115](#).

To authorize metered FortiWeb VMs:

1. Ensure that the FortiWeb VM is registered to the FortiManager. See [Adding devices on page 107](#).
2. In the FortiWeb ADOM, go to *Device Manager > VM Meter*.
3. Select a device then click *Authorize* in the toolbar, right-click on a device then select *Authorize*, or double-click on a device. The *Authorize Device(s)* dialog box opens.
4. On the *Authorize Device* pane, confirm the devices name and serial number.
The *License Type* is *Regular* - points are used based on the volume of traffic. The *Services* - *Security*, *Antivirus*, *IP Reputation* - cannot be deselected.
5. Click *OK* to authorize the device.

Monitoring VMs

Go to *Device Manager > VM Meter*. For prepaid licenses (FortiOS VMs only), your total remaining point balance is shown in the toolbar. For postpaid licenses, the total points used and the billing period are shown.

You can also view details about the individual VMs, including: the device name and serial number, number of virtual CPUs, amount of RAM, service level, license status, volume of traffic used today, and more.

FortiGate chassis devices

Select FortiManager systems can work with the Shelf Manager to manage FortiGate 5050, 5060, 5140, and 5140B chassis. The Shelf Manager runs on the Shelf Management Mezzanine hardware platform included with the FortiGate 5050, 5060, 5140, and 5140B chassis. You can install up to five FortiGate 5000 series blades in the five slots of the FortiGate 5050 ATCA chassis and up to 14 FortiGate 5000 series blades in the 14 slots of the FortiGate 5140 ATCA chassis. For more information on FortiGate 5000 series including Chassis and Shelf manager, see the [Fortinet Document Library](#).

You need to enable chassis management before you can work with the Shelf Manager through the FortiManager system.

To enable chassis management:

1. Go to *System Settings > Advanced > Advanced Settings*. See [Advanced Settings on page 527](#) for more information.
2. Under *Advanced Settings*, select *Chassis Management*.
3. Set the *Chassis Update Interval*, from 4 to 1440 minutes.
4. Click *Apply*.

To add a chassis:

1. Go to *Device Manager > Device & Groups*,
2. Right-click in the tree menu and select *Chassis > Add*. The *Create Chassis* window opens.
3. Complete the following fields, then click *OK*:

Name	Type a unique name for the chassis.
Description	Optionally, type any comments or notes about this chassis.
Chassis Type	Select the chassis type: Chassis 5050, 5060, 5140 or 5140B.
IP Address	Type the IP address of the Shelf Manager running on the chassis.
Authentication Type	Select Anonymous, MD5, or Password from the dropdown list.
Admin User	Type the administrator user name.
Password	Type the administrator password.
Chassis Slot Assignment	You cannot assign FortiGate-5000 series blades to the slot until after the chassis has been added.

To edit a chassis and assign FortiGate 5000 series blade to the slots:

1. Go to *Device Manager > Device & Groups*.
2. Right-click the chassis, and select *Edit*.
3. Modify the fields, except *Chassis Type*.
4. For *Chassis Slot Assignment*, from the dropdown list of a slot, select a FortiGate 5000 series blade to assign it to

the slot. You can select a FortiGate, FortiCarrier, or FortiSwitch unit.



You can only assign FortiSwitch units to slot 1 and 2.

5. Click **OK**.

Viewing chassis dashboard

You can select a chassis from the chassis list in the content pane, and view the status of the FortiGate blades in the slots, power entry module (PEM), fan tray (FortiGate-5140 only), Shelf Manager, and shelf alarm panel (SAP).

Viewing the status of the FortiGate blades

In the *Device Manager* tab, select the Blades under the chassis whose blade information you would like to view.

The following is displayed:

Refresh	Select to update the current page. If there are no entries, Refresh is not displayed.
Slot #	The slot number in the chassis. <ul style="list-style-type: none"> The FortiGate 5050 chassis contains five slots numbered 1 to 5. The FortiGate 5060 chassis contains six slots numbered 1 to 6. The FortiGate 5140 and 5140B chassis contains fourteen slots numbered 1 to 14.
Extension Card	If there is an extension card installed in the blade, this column displays an arrow you can select to expand the display. The expanded display shows details about the extension card as well as the blade.
Slot Info	Indicates whether the slot contains a node card (for example, a FortiGate 5001SX blade) or a switch card (for example, a FortiSwitch 5003 blade) or is empty.
State	Indicates whether the card in the slot is installed or running, or if the slot is empty.
Temperature Sensors	Indicates if the temperature sensors for the blade in each slot are detecting a temperature within an acceptable range. <ul style="list-style-type: none"> OK: All monitored temperatures are within acceptable ranges. Critical: A monitored temperature is too high (usually about 75°C or higher) or too low (below 10°C).
Current Sensors	Indicates if the current sensors for the blade in each slot are detecting a current within an acceptable range. <ul style="list-style-type: none"> OK: All monitored currents are within acceptable ranges. Critical: A monitored current is too high or too low.

Voltage Sensors	Indicates if the voltage sensors for the blade in each slot are detecting a voltage within an acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: All monitored voltages are within acceptable ranges. • <i>Critical</i>: A monitored voltage is too high or too low.
Power Allocated	Indicates the amount of power allocated to each blade in the slot.
Action	Select <i>Activate</i> to turn the state of a blade from <i>Installed</i> into <i>Running</i> . Select <i>Deactivate</i> to turn the state of a blade from <i>Running</i> into <i>Installed</i> .
Edit	Select to view the detailed information on the voltage and temperature of a slot, including sensors, status, and state. You can also edit some voltage and temperature values.
Update	Select to update the slot.

To edit voltage and temperature values:

1. Go to *[chassis name] > Blades* and, in the content pane, select the *Edit* icon of a slot.
The detailed information on the voltage and temperature of the slot including sensors, status, and state is displayed.
2. Select the *Edit* icon of a voltage or temperature sensor.
3. For a voltage sensor, you can modify the *Upper Non-critical*, *Upper Critical*, *Lower Non-critical*, and *Lower Critical* values.
4. For a temperature sensor, you can modify the *Upper Non-critical* and *Upper Critical* values.
5. Select *OK*.

Viewing the status of the power entry modules

You can view the status of the PEMs by going to *[chassis name] > PEM*. The FortiGate 5140 chassis displays more PEM information than the FortiGate 5050.

The following is displayed:

Refresh	Select to update the current page.
PEM	The order numbers of the PEM in the chassis.
Presence	Indicates whether the PEM is present or absent.
Temperature	The temperature of the PEM.
Temperature State	Indicates whether the temperature of the PEM is in the acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: The temperature is within acceptable range.
Threshold	PEM temperature thresholds.
Feed -48V	Number of PEM fuses. There are four pairs per PEM.
Status	PEM fuse status: present or absent.

Power Feed	The power feed for each pair of fuses.
Maximum External Current	Maximum external current for each pair of fuses.
Maximum Internal Current	Maximum internal current for each pair of fuses.
Minimum Voltage	Minimum voltage for each pair of fuses.
Power Available	Available power for each pair of fuses.
Power Allocated	Power allocated to each pair of fuses.
Used By	The slot that uses the power.

Viewing fan tray status (FG-5140 and FG-5140B chassis only)

Go to *[chassis name]* > *Fan Tray* to view the chassis fan tray status.

The following is displayed:

Refresh	Select to update the current page.
Thresholds	Displays the fan tray thresholds.
Fan Tray	The order numbers of the fan trays in the chassis.
Model	The fan tray model.
24V Bus	Status of the 24V Bus: present or absent.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each fan tray.
Fans	Fans in each fan tray.
Status	The fan status. <ul style="list-style-type: none"> OK: It is working normally.
Speed	The fan speed.

Viewing shelf manager status

Go to *[chassis name]* > *Shelf Manager* to view the shelf manager status.

The following is displayed:

Refresh	Select to update the current page.
Shelf Manager	The order numbers of the shelf managers in the chassis.
Model	The shelf manager model.

State	The operation status of the shelf manager.
Temperature	The temperature of the shelf manager.
-48V Bus A	Status of the -48V Bus A: present or absent.
-48V Bus B	Status of the -48V Bus B: present or absent.
Power Allocated	Power allocated to each shelf manager.
Voltage Sensors	Lists the voltage sensors for the shelf manager.
State	Indicates if the voltage sensors for the shelf manager are detecting a voltage within an acceptable range. <ul style="list-style-type: none"> • <i>OK</i>: All monitored voltages are within acceptable ranges. • <i>Below lower critical</i>: A monitored voltage is too low.
Voltage	Voltage value for a voltage sensor.
Edit	Select to modify the thresholds of a voltage sensor.

Viewing shelf alarm panel (SAP) status

You can view the shelf alarm panel (SAP) status for a chassis. The shelf alarm panel helps you monitor the temperature and state of various sensors in the chassis.

Go to `[chassis name] > SAP` to view the chassis SAP status.

The following is displayed:

Presence	Indicates if the SAP is present or absent.
Telco Alarm	Telco form-c relay connections for minor, major and critical power faults provided by the external dry relay Telco alarm interface (48VDC).
Air Filter	Indicates if the air filter is present or absent.
Model	The SAP model.
State	The operation status of the shelf manager.
Power Allocated	Power allocated to the SAP.
Temperature Sensors	The temperature sensors of the SAP
Temperature	The temperature of the SAP read by each sensor.
State	Indicates if the temperature sensors for the SAP are detecting a temperature below the set threshold.
Edit	Select to modify the thresholds of a temperature sensor.

Log and file storage

Logs and files are stored on the FortiManager hard disks. Logs are also temporarily store in the SQL database.

When ADOMs are enabled, settings can be specified for each ADOM that apply only to the devices in it. When ADOMs are disabled, the settings apply to all managed devices.

Data policy and disk utilization settings for devices are collectively called log storage settings. Global log and file storage settings apply to all logs and files, regardless of log storage settings (see [File Management on page 526](#)). Both the global and log storage settings are always active.



These options are only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Disk space allocation

On the FortiManager, the system reserves 5% to 25% of the disk space for system usage and unexpected quota overflow. The remaining 75% to 95% of the disk space is available for allocation to devices.

Reports are stored in the reserved space.

Total Available Disk Size	Reserved Disk Quota
Small Disk (up to 500GB)	The system reserves either 20% or 50GB of disk space, whichever is smaller.
Medium Disk (up to 1TB)	The system reserves either 15% or 100GB of disk space, whichever is smaller.
Large Disk (up to 5TB)	The system reserves either 10% or 200GB of disk space, whichever is smaller.
Very Large Disk (bigger than 5TB)	The system reserves either 5% or 300GB of disk space, whichever is smaller.



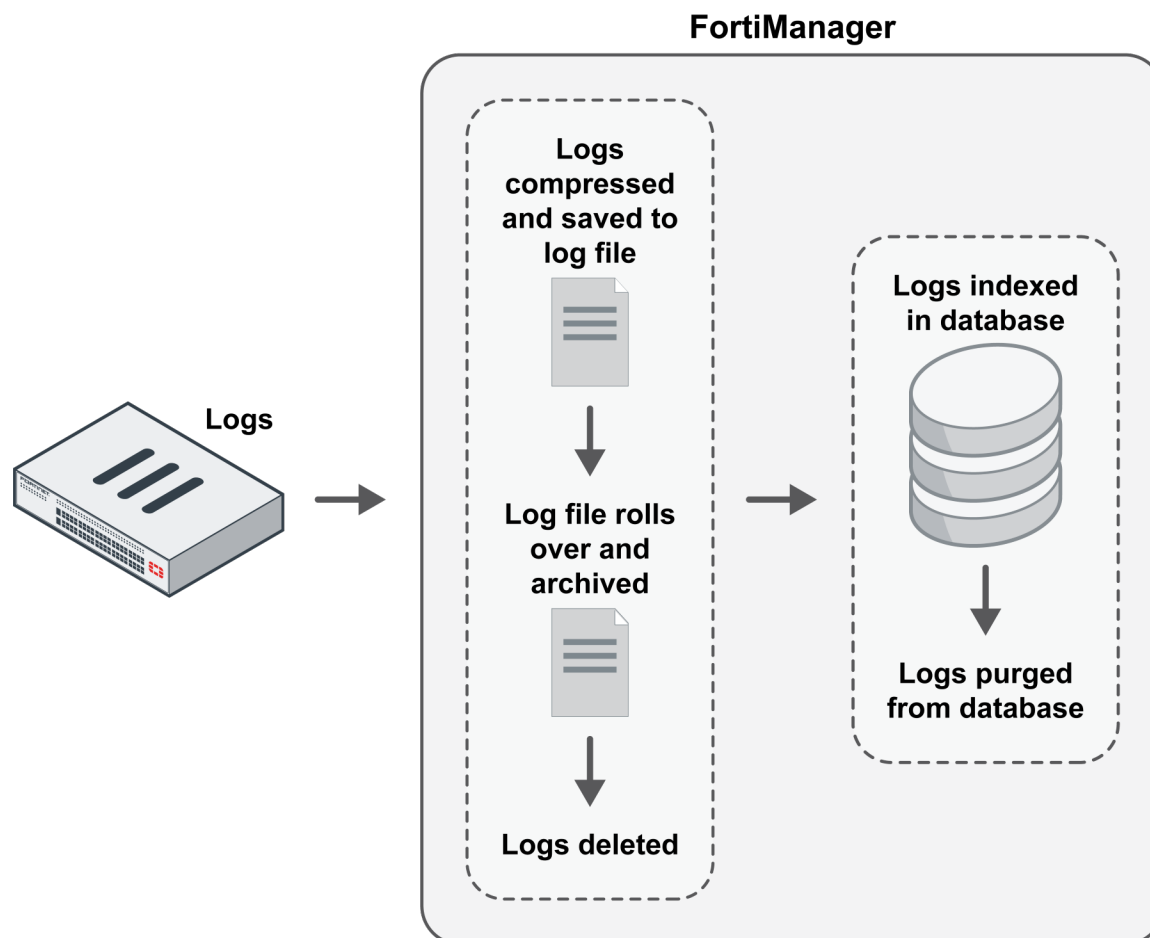
The RAID level you select determines the disk size and the reserved disk quota level. For example, a FortiManager 1000C with four 1TB disks configured in RAID 10 is considered a large disk, so 10%, or 200GB, of disk space is reserved.

Log and file workflow

When devices send logs to a FortiManager unit, the logs enter the following workflow automatically:

1. Logs are compressed and saved in a log file on the FortiManager disks.
When a log file reaches a specified size, FortiManager rolls it over and archives it, and creates a new log file to receive incoming logs. You can specify the size at which the log file rolls over. See [Device logs on page 522](#).

2. Logs are indexed in the SQL database to support analysis.
You can specify how long to keep logs indexed using a data policy. See [Log storage policy on page 208](#).
3. Logs are purged from the SQL database, but remain compressed in a log file on the FortiManager disks.
4. Logs are deleted from the FortiManager disks.
You can specify how long to keep logs using a data policy. See [Log storage policy on page 208](#).



In the indexed phase, logs are indexed in the SQL database for a specified length of time so they can be used for analysis. Indexed, or Analytics, logs are considered online, and details about them can be viewed in the *FortiView*, *NOC*, *Log View*, and *Event Management* modules. You can also generate reports about the logs in the *Reports* pane.

In the compressed phase, logs are compressed and archived in FortiManager disks for a specified length of time for the purpose of retention. Compressed, or Archived, logs are considered offline, and their details cannot be immediately viewed or used to generate reports.

The following table summarizes the differences between indexed and compressed log phases:

Log Phase	Location	Immediate Analytic Support
Indexed	Compressed in log file and indexed in SQL database	Yes. Logs are available for analytic use in <i>FortiView</i> , <i>NOC</i> , <i>Event Management</i> , and <i>Reports</i> .
Compressed	Compressed in log file	No.

Automatic deletion

Logs and files are automatically deleted from the FortiManager unit according to the following settings:

- **Global automatic file deletion**
File management settings specify when to delete the oldest Archive logs, quarantined files, reports, and archived files from the disks, regardless of the log storage settings. See [File Management on page 526](#) for information.
- **Data policy**
Data policies specify how long to store Analytics and Archive logs for each device. When the specified length of time expires, Archive logs for the device are automatically deleted from the FortiManager device's disks.
- **Disk utilization**
Disk utilization settings delete the oldest Archive logs for each device when the allotted disk space is filled. The allotted disk space is defined by the log storage settings. Alerts warn you when the disk space usage reaches a configured percentage.

All deletion policies are active on the FortiManager unit at all times, and you should carefully configure each policy. For example, if the disk fullness policy for a device hits its threshold before the global automatic file deletion policy for the FortiManager unit, Archive logs for the affected device are automatically deleted. Conversely, if the global automatic file deletion policy hits its threshold first, the oldest Archive logs on the FortiManager unit are automatically deleted regardless of the log storage settings associated with the device.

The following table summarizes the automatic deletion policies:

Policy	Scope	Trigger
Global automatic file deletion	All logs, files, and reports on the system	When the specified length of time expires, old files are automatically deleted. This policy applies to all files in the system regardless of the data policy settings associated with devices.
Data policy	Logs for the device with which the data policy is associated	When the specified length of retention time expires, old Archive logs for the device are deleted. This policy affects only Archive logs for the device with which the data policy is associated.
Disk utilization	Logs for the device with which the log storage settings are associated	When the specified threshold is reached for the allotted amount of disk space for the device, the oldest Archive logs are deleted for the device. This policy affects only Archive logs for the device with which the log storage settings are associated.

Logs for deleted devices

When you delete one or more devices from FortiAnalyzer, the raw log files and archive packets are deleted, and the action is recorded in the local event log. However, the logs that have been inserted into the SQL database are not deleted from the SQL database. As a result, logs for the deleted devices might display in the *Log View* and *FortiView* panes, and any reports based on the logs might include results.

The following are ways you can remove logs from the SQL database for deleted devices.

- Rebuild the SQL database for the ADOM to which deleted devices belonged or rebuild the entire SQL database.
- Configure the log storage policy. When the deleted device logs are older than the *Keep Logs for Analytics* setting, they are deleted. Also, when analytic logs exceed their disk quota, the SQL database is trimmed starting with the oldest database tables. For more information, see [Configure log storage on page 209](#).

- Configure global automatic file deletion settings in *System Settings > Advanced > File Management*. When the deleted device logs are older than the configured setting, they are deleted. For more information, see [File Management on page 526](#).



File Management configures global settings that override other log storage settings and apply to all ADOMs.

Log storage policy

The log storage policy affects only the logs and SQL database of the devices associated with the log storage policy. Reports are not affected. See [Disk space allocation on page 205](#).

If ADOMs are enabled, you can view the data policies and disk usage for each ADOM in *System Settings > Storage Info*.

Edit Refresh						
<input type="checkbox"/> Name	Analytics (Actual/Config Days)	Archive (Actual/Config Days)	Max Storage	Analytics Usage (Used/Max)	Archive Usage (Used/Max)	
<input type="checkbox"/> ▼Central Management (2)						
<input type="checkbox"/> FortiCarrier	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> root	0/365	2/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> ▼Other Device Types (10)						
<input type="checkbox"/> FortiAnalyzer	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiAuthenticator	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiCache	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiClient	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiDDoS	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiMail	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiManager	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiSandbox	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> FortiWeb	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	
<input type="checkbox"/> Syslog	0/365	0/365	50 GB	0 MB/30 GB (0%)	0 MB/20 GB (0%)	

The following information and options are available:

Edit	Edit the selected ADOM's log storage policy.
Refresh	Refresh the page.
Search	Enter a search term to search the list.
Name	The name of the ADOM. ADOMs are listed in two groups: <i>Central Management</i> and <i>Other Device Types</i> .
Analytics (Actual/Config Days)	The age, in days, of the oldest Analytics logs (Actual Days), and the number of days Analytics logs will be kept according to the data policy (Config Days).
Archive (Actual/Config Days)	The age, in days, of the oldest Archive logs (Actual Days) and the number of days Archive logs will be kept according to the data policy (Config Days).
Max Storage	The maximum disk space allotted to the ADOM (for both Analytics and Archive logs). See Disk space allocation on page 205 for more information.

**Analytics Usage
(Used/Max)**

How much disk space Analytics logs have used, and the maximum disk space allotted for them.

**Archive Usage
(Used/Max)**

How much disk space Archive logs have used and the maximum disk space allotted for them.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Configure log storage

The log storage policy affects the logs and SQL database of the device associated with the log storage policy.



If you change log storage settings, the new date ranges affect Analytics and Archive logs currently in the FortiManager device. Depending on the date change, Analytics logs might be purged from the database, Archive logs might be added back to the database, and Archive logs outside the date range might be deleted.

To configure log storage settings:

1. Go to *System Settings > Storage Info*.
2. Double-click on an ADOM, right-click on an ADOM and then select *Edit* from the menu, or select the ADOM then click *Edit* in the toolbar. The *Edit Log Storage Policy* pane opens.

Edit Log Storage Policy - ADOM : root

Data Policy			
Keep Logs for Analytics	<input type="text" value="365"/>	<input type="text" value="Days"/>	
Keep Logs for Archive	<input type="text" value="365"/>	<input type="text" value="Days"/>	
Disk Utilization			
Maximum Allowed	<input type="text" value="50"/>	<input type="text" value="GB"/>	Out of Available: 50.0 GB
Analytics : Archive	<input type="text" value="60%"/>	<input type="text" value="40%"/>	<input type="checkbox"/> Modify
Alert and Delete When Usage Reaches	<input type="text" value="100%"/>		

*If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted.

3. Configure the following settings, then click *OK*.

Data Policy

Keep Logs for Analytics

Specify how long to keep Analytics logs.

Keep Logs for Archive

Specify how long to keep Archive logs.
Make sure your setting meets your organization's regulatory requirements.

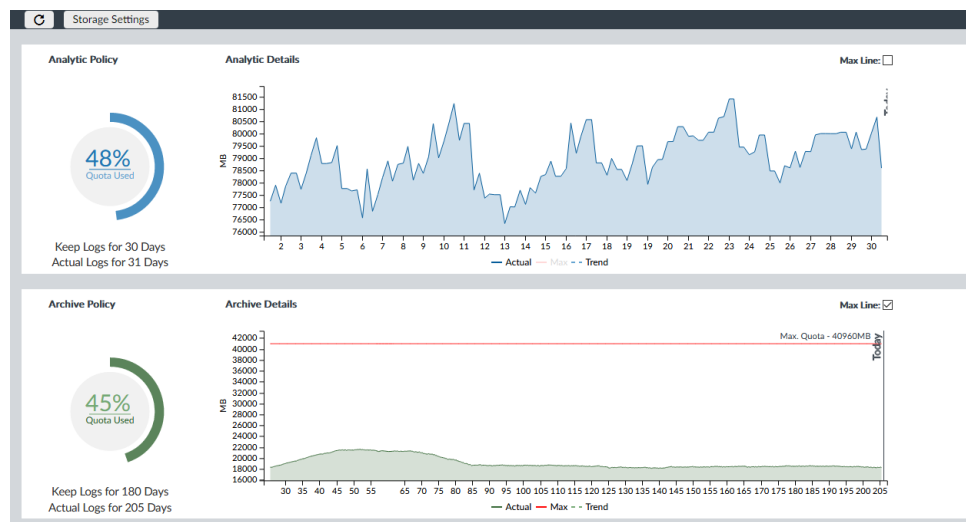
Disk Utilization

Maximum Allowed	Specify the amount of disk space allotted. See also Disk space allocation on page 205 .
Analytics : Archive	Specify the disk space ratio between Analytics and Archive logs. Analytics logs require more space than Archive logs. Click the <i>Modify</i> checkbox to change the setting.
Alert and Delete When Usage Reaches	Specify the percentage of allotted disk space usage that will trigger an alert messages and start automatically deleting logs. The oldest Archive log files or Analytics database tables are deleted first.

Storage statistics

To open the *Storage Statistics* pane, go to *Log View > Storage Statistics*.

The pane shows visualizations of disk space usage for Analytic and Archive logs. The policy diagrams show an overview and the details graphs show disk space usage details.



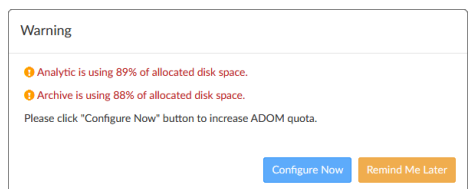
The policy diagram shows the percentage of the disk space quota that is used. Hover your cursor over the diagram to view the used, free, and total allotted disk space. The configured length of time that logs are stored is also shown.

To view or change log storage policies, click *Storage Settings* in the toolbar to open the *Edit Log Storage Policy* dialog box.

The details graph shows the amount disk space used, in MBs, over the time period that the logs are stored for. Click *Max Line* to show a line on the graph for the total space allotted. Hover over a spot in the graph to view the used and available disk space at that specific date and time. Click on a point in the details graph to open a breakdown of the disk space usage by device.

Analytics Storage Statistics - Last 15 Days					
Device Name	Analytics Usage		Average Log Rate (logs/sec)		Peak Log Rate (logs/sec)
FGT37D000000000000	743.1 GB	38.35%	1087.14		1615.27
FG800C000000000000	221.4 MB	0.01%	4.24		35.58
Weixixi_WIFI	3.1 GB	0.16%	4.48		32.80
FG3K2D000000000000	51.3 GB	2.65%	77.29		781.74
FG1K2D000000000000	716.4 GB	36.97%	1048.14		2376.82
FG100D000000000000	423.8 GB	21.87%	619.99		1726.02

When the used quota approaches 100 percent, a warning message displays when accessing the *Storage Statistics* pane.



Click *Configure Now* to open the *Edit Log Storage Policy* dialog box where you can adjust log storage policies to prevent running out of allocated space (see [Configure log storage on page 209](#)), or click *Remind Me Later* to resolve the issue another time.

Policy & Objects

The *Policy & Objects* pane enables you to centrally manage and configure the devices that are managed by the FortiManager unit. This includes the basic network settings to connect the device to the corporate network, antivirus definitions, intrusion protection signatures, access rules, and managing and updating firmware for the devices.

All changes related to policies and objects should be made on the FortiManager device, and not on the managed devices.



If the administrator account you logged on with does not have the appropriate permissions, you will not be able to edit or delete settings, or apply any changes. Instead you are limited to browsing. To modify these settings, see [Administrator profiles on page 85](#).

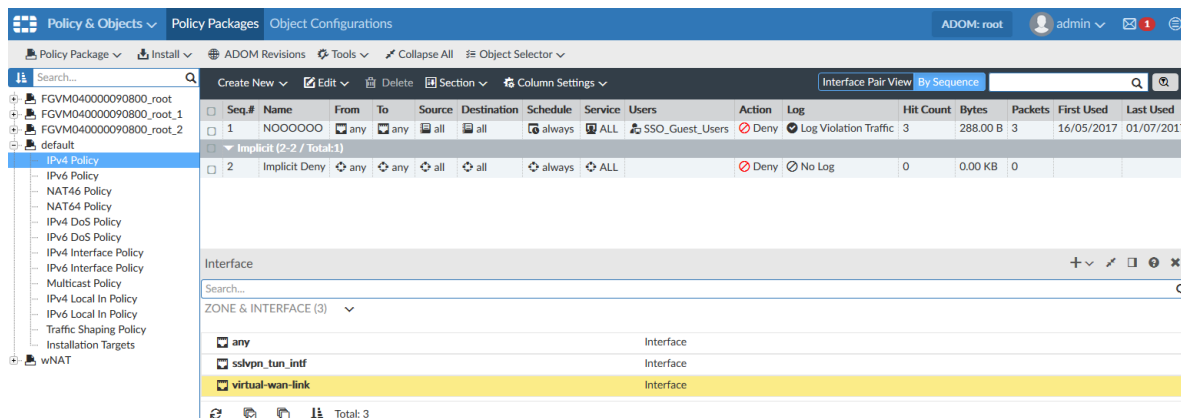


If *Display Policy & Objects in Dual Pane* is enabled, the *Policy Packages* and *Object Configurations* tabs will be shown on the same pane, with *Object Configurations* on the lower half of the screen. See [Display options on page 216](#).



If workspace is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 64](#).

If workflow is enabled, the ADOM must be locked and a session must be started before changes can be made. See [Workflow Mode on page 65](#).



The following tabs are available on the *Policy & Objects* pane by default:

Policy Packages

Click to display the *Policy Packages* pane.

Object Configurations

Click to display the *Object Configurations* pane.

If *Display Policy & Objects in Dual Pane* is enabled, both tabs will be shown on the same pane.

The following options are available on the *Policy Packages* tab:

Policy Package	Click to access the policy package menu. The menu options are the same as the right-click menu options.
Install Wizard	Click to access the Install menu. You can start the Install Wizard where you can install policy packages and device settings. You can also re-install a policy.
ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: <i>Display Options</i> , <i>Find Unused Objects</i> , or <i>Find Duplicate Objects</i> .
Collapse/Expand All	Collapse or expand all the categories in the policy list.
Object Selector	Open the object selector pane on the bottom or right side of the content pane. This option is not available when dual pane is enabled.
Search	The tree menu can be searched and sorted using the search field and sorting button at the top of the menu.

The following options are available on the *Objects Configurations* tab:

ADOM Revisions	Click to create, edit, delete, restore, lock, and unlock ADOM Revisions.
Tools	Click to select one of the following tools from the menu: <i>Display Options</i> , <i>Find Unused Objects</i> , or <i>Find Duplicate Objects</i> .

If workspace is enabled, you can select to lock and edit the policy package in the right-click menu. You do not need to lock the ADOM first. The policy package lock status is displayed in the toolbar.

The following options are available:

Lock Unlock	Select to lock or unlock the ADOM.
Sessions	Click to display the sessions list where you can save, submit, or discard changes made during the session.

About policies

FortiManager provides administrators the ability to customize policies within their organization as they see fit. Typically, administrators may want to customize access and policies based on factors such as geography, specific security requirements, or legal requirements.

Within a single ADOM, administrators can create multiple policy packages. FortiManager provides you the ability to customize policy packages per device or VDOM within a specific ADOM, or to apply a single policy package for all devices within an ADOM. These policy packages can be targeted at a single device, multiple devices, all devices, a single VDOM, multiple VDOMs, or all devices within a single ADOM. By defining the scope of a policy package, an administrator can modify or edit the policies within that package and keep other policy packages unchanged.

FortiManager can help simplify provisioning of new devices, ADOMs, or VDOMs by allowing you to copy or clone existing policy packages.

Policy theory

Security policies control all traffic attempting to pass through a unit between interfaces, zones, and VLAN subinterfaces.

Security policies are instructions that units use to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyzes the packet's source address, destination address, and service (by port number), and attempts to locate a security policy matching the packet.

Security policies can contain many instructions for the unit to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

Policy instructions may include Network Address Translation (NAT), or Port Address Translation (PAT), or they can use virtual IPs or IP pools to translate source and destination IP addresses and port numbers.

Policy instructions may also include Security Profiles, which can specify application-layer inspection and other protocol-specific protection and logging, as well as IPS inspection at the transport layer.

You configure security policies to define which sessions will match the policy and what actions the device will perform with packets from matching sessions.

Sessions are matched to a security policy by considering these features of both the packet and policy:

- Policy Type and Subtype
- Incoming Interface
- Source Address
- Outgoing Interface
- Destination Address
- Schedule and time of the session's initiation
- Service and the packet's port numbers.

If the initial packet matches the security policy, the device performs the configured action and any other configured options on all packets in the session.

Packet handling actions can be *ACCEPT*, *DENY*, *IPSEC*, or *SSL-VPN*.

- *ACCEPT* policy actions permit communication sessions, and may optionally include other packet processing instructions, such as requiring authentication to use the policy, or specifying one or more Security Profiles to apply features such as virus scanning to packets in the session. An *ACCEPT* policy can also apply interface-mode IPsec VPN traffic if either the selected source or destination interface is an IPsec virtual interface.
- *DENY* policy actions block communication sessions, and you can optionally log the denied traffic. If no security policy matches the traffic, the packets are dropped, therefore it is not required to configure a *DENY* security policy in the last position to block the unauthorized traffic. A *DENY* security policy is needed when it is required to log the denied traffic, also called "violation traffic".
- *IPSEC* and *SSL-VPN* policy actions apply a tunnel mode IPsec VPN or SSL VPN tunnel, respectively, and may optionally apply NAT and allow traffic for one or both directions. If permitted by the firewall encryption policy, a tunnel may be initiated automatically whenever a packet matching the policy arrives on the specified network interface, destined for the local private network.

Create security policies based on traffic flow. For example, in a policy for POP3, where the email server is outside of the internal network, traffic should be from an internal interface to an external interface rather than the other way around. It is typically the user on the network requesting email content from the email server and thus the originator of the open connection is on the internal port, not the external one of the email server. This is also important to remember when viewing log messages, as the source and destination of the packets can seem backwards.

Global policy packages

Global policies and objects function in a similar fashion to local policies and objects, but are applied universally to all ADOMs and VDOMs inside your FortiManager installation. This allows users in a carrier, service provider, or large enterprise to support complex installations that may require their customers to pass traffic through their own network.

For example, a carrier or host may allow customers to transit traffic through their network, but do not want their customer to have the ability to access the carrier's internal network or resources. Creating global policy header and footer packages to effectively surround a customer's policy packages can help maintain security.

Global policy packages must be explicitly assigned to specific ADOMs to be used. When configuring global policies, a block of space in the policy table is reserved for *Local Domain Policies*. All of the policies in an ADOM's policy table are inserted into this block when the global policy is assigned to an ADOM.

Display options for policies and objects can be configured in *Policy & Objects > Tools > Display Options*.



Global policies and objects are not supported on all FortiManager platforms. Please review the products' data sheets to determine support.



A global policy license is not required to use global policy packages.

Policy workflow

An administrator will typically carry out two main functions with their devices through FortiManager: provisioning new devices or VDOMs on the network and managing the day-to-day operations of managed devices and VDOMs.

Provisioning new devices

There are multiple steps to provision a new device or VDOM to be managed by the FortiManager unit:

1. In the *Device Manager* pane, create a new VDOM or add a new device.
2. Assign a system template to the provisioned device (optional).
3. In the *Policy & Objects* pane, configure any dynamic objects you wish to assign to the new VDOM or device.
4. Determine how a policy will be defined for the new device: does the new device or VDOM have a new policy package unique to itself, or will the device or VDOM use a package that is implemented elsewhere?
5. Run the *Install Wizard* to install any objects and policies for the new device, or create a new policy package.
6. If the new device uses an existing policy package, modify the installation targets of that package to include the new device.

Day-to-day management of devices

An administrator will often have to modify various objects for the devices they are responsible for managing. A typical set of tasks to manage an already provisioned device will include:

1. Adding, deleting, or editing various objects, such as firewall information, security profiles, user access rights, antivirus signatures, etc.
2. Adding, deleting, or editing all of the policy packages or individual policies within a policy package. This can include changing the order of operation, adding new policies, or modifying information or access permissions in the policy package.
3. Installing updates to devices.

Display options

The policy and objects that are displayed on the *Policy & Objects* pane can be customized, and the *Policy Packages* and *Object Configurations* tabs can be combined onto a single pane.

To adjust the policies and objects that are displayed, go to *Tools > Display Options*.

You can turn the options on or off (visible or hidden). To turn on an option, select the checkbox beside the option name. To turn off an option, clear the checkbox beside the option name. You can turn on all of the options in a category by selecting the checkbox beside the category name. For example, you can turn on all firewall objects by selecting the checkbox beside *Firewall Objects*. You can also turn on all of the categories by clicking the *Check All* button at the bottom of the window.



Various display options are enabled by default and cannot be turned off.

Once turned on, you can configure the corresponding options from the appropriate location on the *Policy & Objects > Object Configurations* pane.

Reset all of the options by clicking the *Reset to Default* button at the bottom of the screen, or reset only the options in a category by clicking the *Reset to Default* button beside the category name.

To convert the module to a single pane:

1. Go to *System Settings > Advanced > Advanced Settings*.
2. Enable Display Policy & Objects in Dual Pane.
3. Click *Apply*.

The *Policy & Objects* pane will now be a single pane that includes both tabs.

Seq. #	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT	Hit Count
1	NOOOOOO	virtual-wan-link vpnmgr_test_hub2spoke vpnmgr_test_mesh sslvpn_tun_intf	any	all	all	always	ALL	SSO_Guest_Users	Deny		Log Violation Traffic		0
2	Test any interface	virtual-wan-link	any	all	all	always	ALL		Accept	default default	Log All Sessions	Disabled	0
▼ Implicit (3-3 / Total:1)													
3	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log		0

Interface	Default Mapping	Per-Device Mapping	Description
▼ Interface (5)			
any		> 0 out of 2	
sslvpn_tun_intf		> 0 out of 2	
virtual-wan-link		> 0 out of 2	
Linkob1		> 0 out of 2	VAP interface
Meshow1		> 0 out of 2	VAP interface
▼ Zone (6)			
vpnmgr_test_hub2spoke		> 0 out of 2	VPN manager auto-generated
vpnmgr_test_mesh		> 0 out of 2	VPN manager auto-generated
vpnmgr_test_spoke2hub		> 0 out of 2	VPN manager auto-generated
vpnmgr_test_hub2spoke		> 0 out of 2	VPN manager auto-generated
vpnmgr_test_mesh		> 0 out of 2	VPN manager auto-generated
vpnmgr_test_spoke2hub		> 0 out of 2	VPN manager auto-generated

Managing policy packages

Policy packages can be created and edited, and then assigned to specific devices in the ADOM. Folders can be created for the policy packages to aid in the organization and management of the packages.

When workspace mode is enabled, policy packages can be individually locked to prevent other administrators from making changes to a package and potentially creating conflicts. See [Concurrent policy package access on page 227](#).



Not all policy and object options are enabled by default. To configure the enabled options, go to *Policy & Objects > Tools > Display Options* and select your required options.



All of the options available from the *Policy Packages* menu can also be accessed by right-clicking anywhere in the policy tree menu.

Create new policy packages

To create a new global policy package:

1. Ensure that you are in the *Global* ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Policy Package* menu select *New Package* or right-click in the tree menu and select *New Package*. The *Create New Policy Package* window opens.
4. Enter a name for the new global policy package.

5. (Optional) Click the *In Folder* button to select a folder.
6. Click *OK* to add the policy package.

To create a new policy package:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Policy Package* menu select *New Package* or right-click in the tree menu and select *New Package*. The *Create New Policy Package* window opens.

4. Configure the following details, then click *OK* to create the policy package.

Name	Enter a name for the new policy package.
In Folder	Optionally, click the <i>In Folder</i> button to select a folder for the package.
Central NAT	Select the <i>Central NAT</i> checkbox to enable <i>Central SNAT</i> and <i>Central DNAT</i> policy types.
Inspection Mode	Select <i>Flow-based</i> (default) or <i>Proxy</i> for the inspection mode. This option is only available for version 5.6 and later ADOMs. For more information on inspection modes, see the FortiOS Handbook , available in the Fortinet Document Library .
NGFW Mode	Select the NGFW mode, <i>Profile-based</i> (default) or <i>Policy-based</i> . This option is only available for version 5.6 and later ADOMs when <i>Inspection Mode</i> is <i>Flow-based</i> .
SSL/SSH Inspection	Select an SSL/SSH inspection type from the dropdown list. This option is only available for version 5.6 and later ADOMs when <i>NGFW Mode</i> is <i>Policy-based</i> .

Create new policy package folders

You can create new policy package folders within existing folders to help you better organize your policy packages.

To create a new policy package folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Policy Package* menu select *New Folder* or right-click in the tree menu and select *New Folder*. The *Create New Policy Folder* window opens.
4. Enter a name for the new policy folder.
5. (Optional) Click the *In Folder* button to nest the new folder inside another folder.
6. Click *OK*. The new policy folder is displayed in the tree menu.

Edit a policy package or folder

Policy packages and policy package folders can be edited and moved as required.

To edit a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package > Edit* from the toolbar, or right-click on the package or folder and select *Edit* from the menu.
4. Edit the settings as required, then click *OK* to apply your changes.



Deselecting *Central NAT* does not delete Central SNAT or Central DNAT entries.

To move a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package > Move* from the toolbar, or right-click on the package or folder and select *Move* from the menu.
4. Change the location of the package or folder as required, then click *OK*.

Clone a policy package

To clone a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select the package or folder in the tree then select *Policy Package > Clone Package* from the toolbar, or right-click on the package or folder and select *Clone Package* from the menu.
4. Edit the name and location of the clone as required.
5. Click *OK* to create the cloned policy package.

Remove a policy package or folder

To remove a policy package or folder:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select the package or folder in the tree menu then select *Policy Package > Delete* from the toolbar, or right-click on the package or folder and select *Delete* from the menu.

Assign a global policy package

Global policy packages can be assigned or installed to specific ADOMs.

Only ADOMs of the same version as the global database or the next higher major release are presented as options for assignment.



The central NAT setting must be consistent between the global policy package and the ADOM to which you are assigning the policy package. Because central NAT is not supported at the global level, you should disable central NAT in all ADOMs to which you are assigning a global policy package.

The inspection-mode setting must also match in the global policy package and the ADOM to which you are assigning the policy package.

To assign a global policy package:

1. Ensure you are in the *Global Database* ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Assignment*. The ADOM assignment list is displayed in the content pane.

Add ADOM Edit ADOM Delete Select All Assign Selected			
ADOMs	Status	ADOM Policy Packages	Action
Gat	Pending changes	All Policy Packages	[Assign]
Got	Up to date	All Policy Packages	[Unassign]
root	Pending changes	All Policy Packages	[Assign]

4. If required, select *Add ADOM* to add an ADOM to the assignment list.
5. In the assignment list, select an ADOM, or click *Select All*.
6. Click *Assign Selected* from the content toolbar. The *Assign* dialog box opens.
7. Select whether you want to assign only used objects or all objects, and if policies will be automatically installed to ADOM devices.
8. Click *OK* to assign the policy package to the selected ADOM or ADOMs.



In the *Assignment* pane you can also edit the ADOM list, delete ADOMs from the list, and assign and unassign ADOMs.

Install a policy package

When installing a policy package, objects that are referenced in the policy will be installed to the target device, and objects that are not referenced will be deleted from the device.



Some objects that are not directly referenced in the policy will also be installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.



Policies within a policy package can be configured to install only on specified target devices. See [Install policies only to specific devices on page 233](#).

To install a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Install* menu, select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can select to install policy package and device settings or install the interface policy only.

For more information on the install wizard, see [Using the Install Wizard to install policy packages and device settings on page 134](#). For more information on editing the installation targets, see [Policy package installation targets on page 224](#).

Reinstall a policy package

You can reinstall a policy package in *Policy & Objects* or *Device Manager*.

To reinstall a policy package:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Perform one of the following actions:
 - Go to *Policy & Objects > Policy Packages*, and select a policy package.
 - Go to *Device Manager*, and select a device.
3. In the toolbar, select *Install > Re-install Policy*.

After data is gathered, the *Re-install Policy Package* window is displayed.

Re-install Policy Package

Device	Policy Package	Validation
FGTM64-96		
root	p1	OK Install Preview Policy Package Diff

[Next >](#) [Cancel](#)

4. (Optional) View a preview of the installation.

- a. Click the *Install Preview* button.

After data is gathered, the *Install Preview* page is displayed.

Install Preview

Device: FGTVM64-96
VDOM: root

```

config webfilter ftgd-local-cat
purge
end
config vpn certificate ca
edit "root_Internal_CA"
set ca "-----BEGIN CERTIFICATE-----
MIIC7jCCAdagAwIBAgIgMUMzODIzNzdCNTFRMzUxOEU1NkJEJERTcwQjREMjYyMzUw
DQYJKoZIhvcNAQEFBQAwKzEWMBQGA1UEChMNRM9ydGluZXQgTHRkLjERMA8GA1UE
AxMIRm9ydGluZXQwHhcNMjYxMjE0MDQ3WhcNMjYxMjE5MDQ3WjArMRYw
FAYDVQQKEw1Gb3J0aW5ldCBMdGQuMREwDwYDVQQDEwhGb3J0aW5ldDCCASlwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAMPasv8MQwRXw7SA5k6vFINXJZ+mydLn
AfxoaxnLDeA7JeWAPbNRtVIGOOd3GoYlxhYToYRnmtZcTBaOmJxKMkwStwvZe+1
-----"

```

[Download](#) [Close](#)

- b. Click the *Download* button to download a text file of the preview information.

- c. Click the *Close* button to close the page and return to the wizard.

5. (Optional) View the difference between the current policy package and the policy in the device.

- a. Click the *Policy Package Diff* button.

After data is gathered, the *Policy Package Diff* page is displayed.

Policy Package Diff (p1)

Summary

Policy - added (1) [\[Details\]](#)

Category	Change Summary	User	
IPv4 Policy	added (1)	admin	[Details]

Policy Object - added (5) changed (3) deleted (106) [\[Details\]](#)

Category	Change Summary	User	
CA Certificate	added (1)	admin	
Local User	deleted (1)	admin	
User Group	deleted (1)	admin	
Device Group	deleted (3)	admin	
Local Category	deleted (2)	admin	
Web Filter Profile	changed (1) deleted (4)	admin	
Address	added (1) changed (1) deleted (1)	admin	
Multicast Address	deleted (5)	admin	
IPv6 Address	deleted (1)	admin	

Close

- b. Click the *Details* links to view details about the changes to the policy, specific policies, and policy objects.
- c. Click *Close* to close the page and return to the wizard.

6. Click *Next*.
7. Click *Install*.

The policy package is reinstalled to the target devices.

Schedule a policy package install

In FortiManager you can create, edit, and delete install schedules for policy packages. The *Schedule Install* menu option has been added to the *Install* wizard when selecting to install policy package and device settings. You can specify the date and time to install the latest policy package changes.

Select the clock icon which is displayed beside the policy package name to create an install schedule. Select this icon to edit or cancel the schedule. When a scheduled install has been configured and is active, hover the mouse over the icon to view the scheduled date and time.

To schedule the install of a policy package to a target device:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Install* menu, select *Install Wizard*. The *Install Wizard* opens.
4. Select *Schedule Install*, and set the install schedule date and time.
5. Select *Next*. In the device selection screen, edit the installation targets as required.
6. Select *Next*. In the interface validation screen, edit the interface mapping as required.
7. Select *Schedule Install* to continue to the policy and object validation screen. In the ready to install screen you can copy the log and download the preview text file.

To edit or cancel an install schedule:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.

3. Click the clock icon next to the policy package name in the *Policy Package* tree. The *Edit Install Schedule* dialog box is displayed.
4. Select *Cancel Schedule* to cancel the install schedule, then select *OK* in the confirmation dialog box to cancel the schedule. Otherwise, edit the install schedule as required and select *OK* to save your changes.

Export a policy package

You can export a policy package to a CSV file.

To export a policy package:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Export*.
Policy packages are exported as CSV files.

Policy package installation targets

The *Installation Targets* pane allows you to view the installation target, config status, policy package status, and schedule install status, as well as edit installation targets for policy package installs.

To view installation targets, go to *Policy & Objects > Policy Packages*. In the tree menu for the policy package, select *Installation Targets*.

The following information is displayed:

Installation Target	The installation target and connection status.
Config Status	See the table below for config status details.
Policy Package Status	See the table below for policy package status details.

The following table identifies the different available config statuses.

Config Status	Icon	Description
Synchronized	Green check ✓	Configurations are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ⚠	Configurations are modified on FortiManager and not synchronized between FortiManager and the managed device.
Auto-update	Green check ✓	Configurations modified on the managed device are auto synced to FortiManager.

Config Status	Icon	Description
Modified (recent auto-updated)	Yellow triangle ▲	Configurations are modified on FortiManager and configurations modified on the managed device are auto synced to FortiManager.
Out of Sync	Red X ✖	Configurations are modified on the managed device and not synced to FortiManager.
Conflict	Red X ✖	When one of the following happens: <ul style="list-style-type: none"> • Install failed • Configurations are modified on both FortiManager and the managed device, and not auto synced to FortiManager.
Unknown	Gray question mark ?	When one of the following happens: <ul style="list-style-type: none"> • Connection goes down • No revision is generated, like added model device

The following table identifies the different available policy package statuses.

Policy Package Status	Icon	Description
Imported	Green check ✓	Policies and objects are imported into FortiManager.
Synchronized	Green check ✓	Policies and objects are synchronized between FortiManager and the managed device.
Modified	Yellow triangle ▲	Policies or objects are modified on FortiManager.
Out of Sync	Red X ✖	Policies or objects are modified on the managed device.
Unknown with policy package name	Gray question mark ?	Configurations of the managed device are retrieved on FortiManager after being imported/installed.
Never Installed	Yellow triangle ▲	No policy package is imported or installed.

The following options are available:

Add	Select to add installation targets (device/group) for the policy package selected. Select the add icon beside <i>Device/Group</i> to select devices.
------------	--

Delete	Select to delete the selected entries from the installation target for the policy package selected.
Install	Select an entry in the table and, from the <i>Install</i> menu, select <i>Install Wizard</i> or <i>Re-install Policy</i> .
Search	Use the search field to search installation targets. Entering text in the search field will highlight matches.

Perform a policy consistency check

The policy check tool allows you to check all policy packages within an ADOM to ensure consistency and eliminate conflicts that may prevent your devices from passing traffic. This allows you to optimize your policy sets and potentially reduce the size of your databases.

The check will verify:

- Object duplication: two objects that have identical definitions
- Object shadowing: a higher priority object completely encompasses another object of the same type
- Object overlap: one object partially overlaps another object of the same type
- Object orphaning: an object has been defined but has not been used anywhere.

The policy check uses an algorithm to evaluate policy objects, based on the following attributes:

- The source and destination interface policy objects
- The source and destination address policy objects
- The service and schedule policy objects.

To perform a policy check:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To perform a new consistency check, select *Perform Policy Consistency Check*, then click *OK*.
A policy consistency check is performed, and the results screen is shown.

To view the results of the last policy consistency check:

1. Select the ADOM for which you performed a consistency check.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package or folder, and from the *Policy Package* menu, select *Policy Check*. The *Policy Consistency Check* dialog box opens.
4. To view the results of the most recent consistency check, select *View Last Policy Consistency Check Result*, then click *OK*.
The *Policy Consistency Check* window opens, showing the results of the last policy consistency check.

View logs related to a policy rule

After you add a FortiAnalyzer device to FortiManager by using the Add FortiAnalyzer wizard, you can view the logs that it receives. In the *Policy & Objects* pane, you can view logs related to the UUID for a policy rule. You can also use the UUID to search related policy rules.

See also [Adding FortiAnalyzer devices on page 119](#).

To view logs related to a policy rule:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. From the *Column Settings* menu in the toolbar, select *UUID*.
The UUID column is displayed.
4. Select a policy package.
5. In the content pane, right click a number in the *UUID* column, and select *View Log*.
The *View Log by UUID: <UUID>* window is displayed and lists all of the logs associated with the policy ID.

Concurrent policy package access

Concurrent policy package access is controlled by enabling or disabling the workspace function. Concurrent access is enabled by default. To prevent multiple administrators from making changes to a policy package at the same time and causing conflicts, the workspace function must be enabled.

When workspace mode is enabled, concurrent package access is disabled. An administrator must lock the package before they can make changes to it, and only one administrator can hold the lock at one time. Other administrators will have read-only access to the package. Any changes that an administrator makes to a package must be saved, by clicking *Save* in the toolbar, prior to unlocking the package for them to be applied, otherwise the changes will be discarded.

When workspace is disabled, concurrent policy package access is enabled, and multiple administrators can log in and make changes to the same package at the same time.

To enable workspace mode, and disable concurrent package access:

1. Enter the following CLI commands:

```
config system global
    set workspace-mode normal
end
```

To disable workspace mode, and enable concurrent package access:

1. Enter the following CLI commands:

```
config system global
    set workspace-mode disabled
Warning: disabling workspaces may cause some logged in users to lose their unsaved data.
Do you want to continue? (y/n) y
end
```



After changing the workflow mode, your session will end and you will be required to log back in to the FortiManager.

Locking a policy package

If workspace is enabled, you must lock a policy package prior to performing changes to it.

When locked, a padlock icon will be shown next to the policy package name in the tree menu. The icon will be green if you locked the package, or red if another administrator has locked the package.

The lock will be removed when an administrator either unlocks the package, or logs out of the FortiManager.

To lock a policy package:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Do one of the following:
 - Select a policy package, or a policy type in the package from the tree menu, then select *Policy Package > Lock* from the toolbar.
 - Right-click anywhere inside a policy package on the tree menu and select *Lock* from the right-click menu.

The policy package will be locked, allowing you to make changes to it and preventing other administrators from making any changes to it.

To unlock a policy package:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. Do one of the following:
 - Select a locked policy package, or a policy type in the package from the tree menu, then select *Policy Package > Unlock* from the toolbar.
 - Right-click anywhere inside the policy package on the tree menu and select *Unlock* from the right-click menu.

The policy package will be unlocked, allowing other administrators to lock the package and make changes to it. If there are unsaved changes to the package, a dialog box will give you the option of saving or discarding your changes before unlocking the package.

Managing policies

Policies in policy packages can be created and managed by selecting an ADOM, and then selecting the policy package whose policies you are configuring. Sections can be added to the policy list to help organize your policies, and the policies can be listed in sequence, or by interface pairs.

On the *Policy & Objects > Policy Packages* pane, the tree menu lists the policy packages and the policies in each policy package. In the following example, the *default* policy package is displayed with its policies, such as IPv4 Policy,

IPv6 Policy, and so on. The policies that are displayed for each policy package are controlled by the display options. See [Display options on page 216](#) for more information.

Seq.#	Name	From	To	Source	Destination	Schedule	Service	Users	Action	Security Profiles	Log	NAT	Comments	Created Time	Last Modified
1	Flexo	sd-wan	sd-wan	all	all	always	ALL	guest, SSO_Guest_Users, Guest-group, all	Deny		Log Violation Traffic			2018-05-02 12:04:36	admin/2018-05-02 12:04:36
2	Roberto	any	any	all	ntp.org-Web, ntp.org-NTP	always			IPsec		No Log			2018-05-02 12:05:50	admin/2018-05-02 12:05:50
3	Unit 2013	any	any	all	all	always	ALL		Accept		Log All Sessions	Enabled		2018-05-02 12:07:22	admin/2018-05-02 12:07:22
4	Implicit Deny	any	any	all	all	always	ALL		Deny		No Log				

You can configure the following policies for a policy package:

IP policies
NAT policies
Proxy policy
Central SNAT

Central DNAT
DoS policy
Interface policy
Multicast policy

Local in policy
Traffic shaping policy

Various options are also available from column specific right-click menus, for more information see [Column options on page 229](#).

For more information about policies, see the *FortiOS Handbook* available in the [Fortinet Document Library](#).



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 64](#).



Not all policy and object options are enabled by default. To configure the enabled options, from the *Tools* menu, select *Display Options*.



Section view will be disabled if one or more policies are using the *Any* interface, or if one or more policies are configured with multiple source or destination interfaces.

Column options

The visible columns can be adjusted, where applicable, using the *Column Settings* menu in the content pane toolbar. The columns and columns filters available are dependent on the policy and the ADOM firmware version.

Click and drag an applicable column to move it to another location in the table.

Policy search and filter

Go to *Policy & Objects > Policy Packages*, and use the search box to search or filter policies for matching rules or objects.

The default *Simple Search* will highlight text that matches the string entered in the search field.

To add column filters:

1. Select *Column Filter* from the search field dropdown menu.
2. Do either of the following:
 - a. Right-click on a specific value in any column and select *Add Filter* (equals or not equals) from the menu.or
 - a. Click *Add Filter*, then select a column heading from the list.
 - b. Select from the available values in the provided list. Select *Or* to add multiple values, or select *Not* to remove any policies that contain the selected value from the results.

Multiple filters can be added.

3. Click *Go* to filter the list.

Policy hit count

You can use FortiManager to view FortiGate policy hit counters. You must enable policy hit counts before you can view the information.

When the policy hit counter is reset on the FortiGate, FortiManager subtracts the amount from its hit counters too.

To enable policy hits:

1. Go to *System Settings > Advanced Settings*.
2. Beside *Policy Hit Count*, select *Enable*.

To view policy hit counts:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Package*.
3. In the tree menu for a policy package, select a policy. The content pane for the policy is displayed.
4. View the *Hit Count* column.

Creating policies

To create a new policy:

Policy creation varies depending on the type of policy that is being created. See the following section that corresponds to the type of policy you are creating for specific instructions on creating that type of policy.



Policy creation will vary by ADOM version.



For information on creating policies, see the *FortiOS Handbook*, available in the [Fortinet Document Library](#).

To insert a policy:

Generic policies can be inserted above or below the currently selected policy. From the *Create New* menu, select *Insert Above* or *Insert Below*. By default, new policies will be inserted at the bottom of the list.

Editing policies

Policies can be edited in a variety of different way, often directly on the policy list.

To edit a policy:

Select a policy and select *Edit* from the *Edit* menu, or double-click on a policy, to open the *Edit Policy* pane.

You can also edit a policy inline using the object pane (either the *Object Selector* frame or the *Object Configurations* pane when dual pane is enabled), the right-click menu, and by dragging and dropping objects. See [Object selector on page 232](#) and [Drag and drop objects on page 233](#).

The right-click menu changes based on the cell or object that is clicked on.

To clone a policy:

Select a policy, and from the *Edit* menu, select *Clone*. The *Clone Policy* dialog box opens with all of the settings of the original policy. Edit the settings as required and select *OK* to create the clone.

To copy, cut, or paste a policy or object:

You can copy, cut, and paste policies. Select a policy, and from the *Edit* menu, select *Cut* or *Copy*. When pasting a copied or cut policy, you can insert it above or below the currently selected policy.

You can also copy, cut, and paste objects within a policy. Select an object in a cell, or select multiple objects using the control key, then right-click and select *Copy* or *Cut*. Copied or cut objects can only be pasted into appropriate cells; an address cannot be pasted into a service cell for example.



A copied or cut policy or object can be pasted multiple times without having to be recopied.

To delete a policy:

You can delete a policy. Select a policy, and from the *Edit* menu, select *Delete*.

To add a section:

You can use sections to help organize your policy list. Policies can also be appended to sections.

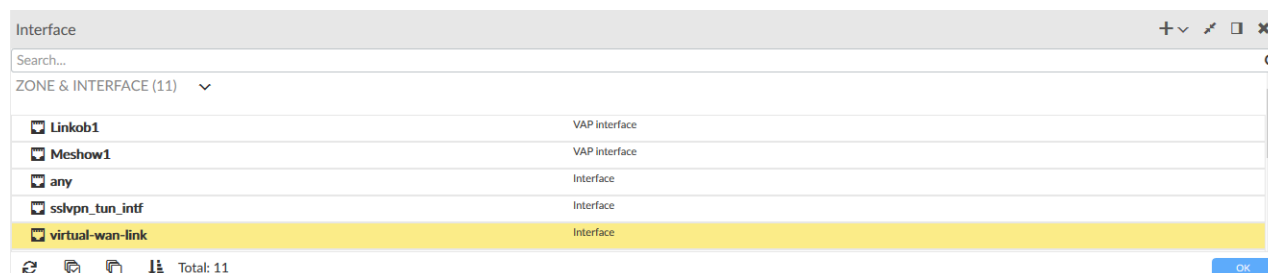
Select a policy, and from the *Section* menu, click *Add*. Type a section name, and click *OK* to add a section to the currently selected policy.

Object selector

The *Object Selector* frame opens when a cell in the policy list is selected.



The *Object Selector* frame is only available when *Display Policy & Objects in Dual Pane* is disabled. See [Display options on page 216](#).



Create New	Click the create new dropdown list, then select the object type to make a new object. See Create a new object on page 262 .
Collapse / Expand All	Expand or collapse all of the object groups shown in the pane.
Dock to bottom / right	Move the <i>Object Selector</i> frame to the bottom or right side of the content pane.
Close	Close the <i>Object Selector</i> frame.
Search	Enter a search term to search the object list.
Refresh	Refresh the list.
Select All	Select all objects in the list.
Deselect All	Deselect all objects in the list.
Sort	Sort the object list alphabetically.

Objects can be added or removed from the selected cell by clicking on them, and then selecting *OK* to apply the change and close the *Object Selection* pane.

Objects can also be dragged and dropped from the pane to applicable, highlighted cells in the policy list.

Right-click on an object in the pane to *Edit* or *Clone* the object, and to see where it is used. See [Edit an object on page 265](#) and [Clone an object on page 266](#).

Drag and drop objects

On the *Policy & Objects > Policy Packages* pane, objects can be dragged and dropped from the object pane, and can also be dragged from one cell to another, without removing the object from the original cell.

One or more objects can be dragged at the same time. When dragging a single object, a box beside the pointer will display the name of the object being dragged. When dragging multiple objects, the box beside the pointer will show a count of the number of objects that are being dragged. To select multiple objects, click them while holding the control key on your keyboard.

The cells or columns that the object or objects can be dropped into will be highlighted in the policy package pane. After dropping the object or objects into a cell or column, the object will immediately appear in the cell as part of the policy, or in all the cells of that column.

Install policies only to specific devices

Policies can be configured to install only to specific installation targets within the policy package. This allows a single policy package to be applied to multiple different types of devices. For example, FortiGate and FortiWiFi devices can share the same policy, even though FortiGate devices do not have WiFi interfaces.

To install a policy only to specific devices:

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu, select the policy package
4. Select *Column Settings > Install On* from the content pane toolbar. The *Install On* column is not shown by default.
5. Click *Installation Targets* in the *Install On* column of the policy that will be applied to specific devices.
6. In the *Object Selector* frame, select the devices that the policy will be installed on (see [Policy package installation targets on page 224](#)), then click *OK*.

The policy will now be installed only on the selected installation targets, and not the other devices to which the policy package is assigned.

Configuring policy details

Various policy details can be configured directly from the policy tables, such as the policy schedule, service, action, security profiles, and logging.

To edit a policy schedule with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Schedule* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy schedule with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects > Schedules*.
5. Locate the schedule object, then drag and drop the object onto the cell in the *Schedule* column for the policy that you want to change.

To edit a policy service with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Service* column, click the cell in the policy that you want to edit. The *Object Selector* frame opens.
5. In the *Object Selector* frame, locate the service object, and then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit a policy service with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
5. Locate the service object, then drag and drop the object onto the cell in the *Service* column for the policy that you want to change.

To edit a services object:

1. Go to *Policy & Objects > Object Configuration*.
2. In the tree menu, go to *Firewall Objects > Services*. The services objects are displayed in the content pane.
3. Select a services object, and click *Edit*. The *Edit Service* dialog box is displayed.
4. Configure the following settings, then click *OK* to save the service. The custom service will be added to the available services.

Name	Edit the service name as required.
Comments	Type an optional comment.
Service Type	Select <i>Firewall</i> or <i>Explicit Proxy</i> .
Show in service list	Select to display the object in the services list.
Category	Select a category for the service.
Protocol Type	Select the protocol from the dropdown list. Select one of the following: <i>TCP/UDP/SCTP, ICMP, ICMP6, or IP.</i>

IP/FQDN	Type the IP address or FQDN. This menu item is available when <i>Protocol</i> is set to <i>TCP/UDP/SCTP</i> . You can then define the protocol, source port, and destination port in the table.
Type	Type the service type in the text field. This menu item is available when <i>Protocol</i> is set to <i>ICMP</i> or <i>ICMP6</i> .
Code	Type the code in the text field. This menu item is available when <i>Protocol</i> is set to <i>ICMP</i> or <i>ICMP6</i> .
Protocol Number	Type the protocol number in the text field. This menu item is available when <i>Protocol Type</i> is set to <i>IP</i> .
Advanced Options	For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
check-reset-range	Configure ICMP error message verification. <ul style="list-style-type: none"> <code>disable</code>: The FortiGate unit does not validate ICMP error messages. <code>strict</code>: If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) TCP(C,D) header, then if FortiManager can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If it is enabled, the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the <code>anti-replay</code> option checks packets. <code>default</code>: Use the global setting defined in <code>system global</code>. This field is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> . This field is not available if <i>explicit-proxy</i> is enabled.
Color	Click the icon to select a custom, colored icon to display next to the service name.
session-ttl	Type the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Type 0 to use either the <code>per-policy session-ttl</code> or <code>per-VDOM session-ttl</code> , as applicable. This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
tcp-halfclose-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type 0 to use the global setting defined in <code>system global</code> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .
tcp-halfopen-timer	Type how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Type 0 to use the global setting defined in <code>system global</code> . This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i> .

tcp-timewait-timer	<p>Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the "...TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request."</p> <p>Reducing the length of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster, which means that more new sessions can be opened before the session limit is reached.</p> <p>The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds. Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>
udp-idle-timer	<p>Type the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds.</p> <p>Type 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <i>Protocol</i> is <i>TCP/UDP/SCTP</i>.</p>

To edit a policy action:

1. Select desired policy type in the tree menu.
2. Select the policy, and from the *Edit* menu, select *Edit*.
3. Set the *Action* option, and click *OK*.

To edit policy logging:

1. Select desired policy type in the tree menu.
2. Right-click the *Log* column, and select options from the menu.

To edit policy security profiles with dual pane disabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the *Security Profiles* column, click the cell in the policy that you want to edit. The *Object Selector* frame is displayed.
5. In the *Object Selector* frame, locate the profiles, then drag and drop the object onto the cell in the *Security Profiles* column for the policy that you want to change.
6. Click *OK* to close the *Object Selector* frame.

To edit policy security profiles with dual pane enabled:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. In the tree menu for a policy package, select a policy type. The policies are displayed in the content pane.
4. In the object pane, go to *Security Profiles*.
5. Locate the profile object, then drag and drop the object onto the cell in the *Security Profiles* column for the policy that you want to change.



The policy action must be *Accept* to add security profiles to the policy.

IP policies

The section describes how to create new IPv4 and IPv6 policies.

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over to IPv6, but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.



On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

To create a new IPv4 or IPv6 policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.

Create New IPv4 Policy

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/>
Outgoing Interface	<input type="text" value="any"/>
Source Address	<input type="text" value="all"/>
Source User	<input type="text" value="+"/>
Source User Group	<input type="text" value="+"/>
Source Device	<input type="text" value="+"/>
Internet Service	<input type="checkbox"/> OFF
Destination Address	<input type="text" value="all"/>
Service	<input type="text" value="ALL"/>
Schedule	<input type="text" value="always"/>
Action	<input checked="" type="radio"/> Deny <input type="radio"/> Accept <input type="radio"/> IPSEC
Log Traffic	<input checked="" type="checkbox"/> Log Violation Traffic <input type="checkbox"/> Generate Logs when Session Starts
Description	<input type="text"/>

Advanced Options >

5. Enter the following information:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Incoming Interface	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. Select the remove icon to remove values. New objects can be created by clicking the <i>Create New</i> icon in the <i>Object Selector</i> frame. See Create a new object on page 262 for more information.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.
Source User	Select source users.
Source User Group	Select source user groups.
Source Device	Select source devices, device groups, and device categories.
Internet Service	Turn internet service on or off. This option is only available for IPv4 policies.
Destination Internet Service	Select internet services. This option is only available when <i>Internet Service</i> is on.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is only available when <i>Internet Service</i> is off.
Service	Select services and service groups. This option is only available when <i>Internet Service</i> is off.
Schedule	Select schedules, one time or recurring, and schedule groups.
Application	Select applications. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> ; see Create new policy packages on page 217 .
URL Category	Select URL categories. This option is only available when <i>NGFW Mode</i> is <i>Policy-based</i> ; see Create new policy packages on page 217 .
Action	Select an action for the policy to take: <i>ACCEPT</i> , <i>DENY</i> , or <i>IPSEC</i> . <i>IPSEC</i> is not available for IPv6 policies.
Log Traffic	When the <i>Action</i> is <i>DENY</i> , select <i>Log Violation Traffic</i> to log violation traffic. When the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> , select one of the following options: <ul style="list-style-type: none"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i>

Generate Logs when Session Starts	Select to generate logs when the session starts.
Capture Packets	Select to capture packets. This option is available when the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> , and <i>Log Security Events</i> or <i>Log All Sessions</i> is selected
NAT	Select to enable NAT. If enabled, select <i>Use Destination Interface Address</i> or <i>Dynamic IP Pool</i> , and select <i>Fixed Port</i> if required. If <i>Dynamic IP Pool</i> is selected, select pools. This option is available when the <i>Action</i> is <i>ACCEPT</i> , and when <i>NGFW Mode</i> is <i>Profile-based</i> ; see Create new policy packages on page 217 .
VPN Tunnel	Select a VPN tunnel dynamic object from the dropdown list. Select to allow traffic to be initiated from the remote site. This option is available when the <i>Action</i> is <i>IPSEC</i> .
Security Profiles	Select to add security profiles or profile groups. This option is available when the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> . The following profile types can be added: <ul style="list-style-type: none"> • Antivirus Profile • Web Filter Profile • Application Control • IPS Profile • Email Filter Profile • DLP Sensor • VoIP Profile • ICAP Profile • SSL/SSH Inspection • Web Application Firewall • DNS Filter • CASI • Proxy Options • Profile Group (available when <i>Use Security Profile Group</i> is selected)
Shared Shaper	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Reverse Shaper	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> and at least one forward traffic shaper is selected.
Per-IP Shaper	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> .
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.

Advanced Options

Configure advanced options, see [Advanced options](#).

For more information on advanced option, see the *FortiOS CLI Reference*.

- Click **OK** to create the policy. You can select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Advanced options

Option	Description	Default
auth-cert	HTTPS server certificate for policy authentication (IPv4 only).	none
auth-path	Enable or disable authentication-based routing (IPv4 only).	disable
auth-redirect-addr	HTTP-to-HTTPS redirect address for firewall authentication (IPv4 only).	none
auto-asic-offload	Enable or disable policy traffic ASIC offloading.	enable
block-notification	Enable or disable block notification (IPv4 only).	disable
captive-portal-exempt	Enable or disable exemption of captive portal (IPv4 only).	disable
custom-log-fields	Select the custom log fields from the dropdown list.	none
delay-tcp-npu-session	Enable or disable TCP NPU session delay in order to guarantee packet order of 3-way handshake (IPv4 only).	disable
diffserv-forward	Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic.	disable
diffserv-reverse	Enable or disable application of the DSCP value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> .	disable
diffservcode-forward	Type the DSCP value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev	Type the DSCP value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
disclaimer	Enable or disable user authentication disclaimer (IPv4 only).	disable
dscp-match	Enable or disable DSCP check.	disable
dscp-negate	Enable or disable negate DSCP match.	disable
dscp-value	Enter the DSCP value.	000000
dsri	Enable or disable DSRI (Disable Server Response Inspection).	disable
dstaddr-negate	Enable or disable negated destination address match.	disable
firewall-session-dirty	Packet session management, either <i>check-all</i> or <i>check-new</i> .	check-all

Option	Description	Default
fsso-agent-for-ntlm	Select the FSSO agent for NTLM from the dropdown list (IPv4 only).	none
identity-based-route	Name of identity-based routing rule (IPv4 only).	none
internet-service-negate	When enabled, Internet services match against any Internet service EXCEPT the selected Internet service (IPv4 only).	disable
learning-mode	Enable or disable learning mode for policy (IPv4 only).	disable
match-vip	Enable or disable match DNATed packet (IPv4 only).	disable
natinbound	Enable or disable policy NAT inbound.	disable
natip	Type the NAT IP address in the text field (IPv4 only).	0.0.0.0
natoutbound	Enable or disable policy NAT outbound.	disable
np-acceleration	Enable or disable UTM Network Processor acceleration.	enable
ntlm	Enable or disable NTLM authentication (IPv4 only).	disable
ntlm-enabled-browsers	Type a value in the text field (IPv4 only).	none
ntlm-guest	Enable or disable NTLM guest (IPv4 only).	disable
outbound	Enable or disable policy outbound.	disable
permit-any-host	Enable to accept UDP packets from any host (IPv4 only).	disable
permit-stun-host	Enable to accept UDP packets from any STUN host (IPv4 only).	disable
radius-mac-auth-bypass	Enable MAC authentication bypass. The bypassed MAC address must be received from RADIUS server.	disable
redirect-url	URL redirection after disclaimer/authentication (IPv4 only).	none
replacemsg-override-group	Specify authentication replacement message override group.	none
rtp-addr	Select the RTP address from the dropdown list (IPv4 only).	none
rtp-nat	Enable to apply source NAT to RTP packets received by the firewall policy (IPv4 only).	disable
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers (IPv4 only).	disable
schedule-timeout	Enable to force session to end when policy schedule end time is reached (IPv4 only).	disable
send-deny-packet	Enable to send a packet in reply to denied TCP, UDP or ICMP traffic.	disable
service-negate	Enable or disable negated service match.	disable
session-ttl	Type a value for the session time-to-live (TTL) from 300 to 604800, or type 0 for no limitation.	0

Option	Description	Default
srcaddr-negate	Enable or disable negated source address match.	disable
ssl-mirror	Enable or disable SSL mirror.	disable
ssl-mirror-intf	Mirror interface name.	none
tags	Applied object tags.	none
tcp-mss-receiver	Type a value for the receiver's TCP MSS.	0
tcp-mss-sender	Type a value for the sender's TCP MSS.	0
tcp-session-without-syn	Enable or disable creation of TCP session without SYN flag. <ul style="list-style-type: none"> all - Enable TCP session without SYN. data-only - Enable TCP session data only. disable - Disable TCP session without SYN. 	disable
timeout-send-rst	Enable sending a TCP reset when an application session times out.	disable
vlan-cos-fwd	Type the VLAN forward direction user priority.	255
vlan-cos-rev	Type the VLAN reverse direction user priority.	255
wanopt	Enable or disable WAN optimization (IPv4 only).	disable
wanopt-detection	WAN optimization auto-detection mode (IPv4 only).	active
wanopt-passive-opt	WAN optimization passive mode options. This option decides what IP address will be used to connect server (IPv4 only).	default
wanopt-peer	WAN optimization peer (IPv4 only).	none
wanopt-profile	WAN optimization profile (IPv4 only).	none
wccp	Enable or disable Web Cache Communication Protocol (WCCP) (IPv4 only).	disable
webcache	Enable or disable web cache (IPv4 only).	disable
webcache-https	Enable or disable web cache for HTTPS (IPv4 only).	disable
wssso	Enable or disable WiFi Single Sign-On (IPv4 only).	enable

Virtual wire pair policy

The section describes how to create virtual wire pair policies. Before you can create a policy, you must create a virtual wire pair. See [Configuring virtual wire pairs on page 275](#).



You must display the option before you can set it. On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Virtual Wire Pair Policy* checkbox to display this option.

To create a virtual wire pair policy:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Virtual Wire Pair Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Enter the following information, then click *OK* to create the policy:

Name	Enter a unique name for the policy. Each policy must have a unique name.
Virtual Wire Pair Interface	Select an interface. You can type the name of the interface to search for it in the list.
Virtual Wire Pair	Select an arrow to indicate the flow of traffic between ports.
Source Address	Select source addresses.
Source User	Select source users.
Source User Group	Select source user groups.
Source Device	Select source devices, device groups, and device categories.
Internet Service	Toggle <i>ON</i> to enable Internet service. Toggle <i>OFF</i> to disable Internet service.
Destination Internet Service	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is available when <i>Internet Service</i> is <i>ON</i> .
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups. This option is available when <i>Internet Service</i> is <i>OFF</i> .
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>Deny</i> or <i>Accept</i> .
Log Traffic	When the <i>Action</i> is <i>DENY</i> , select <i>Log Violation Traffic</i> to log violation traffic. When the <i>Action</i> is <i>ACCEPT</i> , select one of the following options: <ul style="list-style-type: none"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i>
Generate Logs when Session Starts	Select to generate logs when the session starts.
Capture Packets	Select to capture packets. This option is available when the <i>Action</i> is <i>ACCEPT</i> and <i>Log Security Events</i> or <i>Log All Sessions</i> is selected

Security Profiles	<p>Select to add security profiles or profile groups.</p> <p>This option is available when <i>Action</i> is <i>Accept</i>.</p> <p>The following profile types can be added:</p> <ul style="list-style-type: none"> • AntiVirus Profile • Web Filter Profile • Application Control • IPS Profile • Email Filter Profile • DLP Sensor • VoIP Profile • ICAP Profile • SSL/SSH Inspection • Web Application Firewall • DNS Filter • Proxy Options • Profile Group (available when <i>Use Security Profile Group</i> is selected)
Shared Shaper	<p>Select traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i>.</p>
Reverse Shaper	<p>Select traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i> and at least one forward traffic shaper is selected.</p>
Per-IP Shaper	<p>Select per IP traffic shapers.</p> <p>This option is available if the <i>Action</i> is <i>ACCEPT</i> or <i>IPSEC</i>.</p>
Description	<p>Add a description of the policy, such as its purpose, or the changes that have been made to it.</p>
Advanced Options	<p>Configure advanced options, see Advanced options on page 240.</p> <p>For more information on advanced option, see the <i>FortiOS CLI Reference</i>.</p>

NAT policies

Use NAT46 policies for IPv6 environments where you want to expose certain services to the public IPv4 Internet. You will need to configure a virtual IP to permit the access.

Use NAT64 policies to perform network address translation (NAT) between an internal IPv6 network and an external IPv4 network.

The NAT46 Policy tab allows you to create, edit, delete, and clone NAT46 policies. The NAT64 Policy tab allows you to create, edit, delete, and clone NAT64 policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *NAT46 Policy* and *NAT64 Policy* checkboxes to display these options.

To create a NAT46 or NAT64 policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *NAT46 Policy* or *NAT64 Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

Incoming Interface	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>ACCEPT</i> , or <i>DENY</i> .
Log Allowed Traffic	Select to log allowed traffic.
NAT	NAT is enabled by default for this policy type when the <i>Action</i> is <i>ACCEPT</i> . <i>Use Destination Interface Address</i> is selected by default. Select <i>Fixed Port</i> if required.
Traffic Shaping	Select traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
Reverse Traffic Shaping	Select traffic shapers. This option is available if at least one forward traffic shaper is selected.
Per-IP Traffic Shaping	Select per IP traffic shapers. This option is available if the <i>Action</i> is <i>ACCEPT</i> .
Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	
permit-any-host	Enable to accept UDP packets from any host.
tags	Applied object tags.
tcp-mss-receiver	Type a value for the receiver's TCP MSS.
tcp-mss-sender	Type a value for the sender's TCP MSS.

Proxy policy

The section describes how to create web, FTP, and WAN Opt proxy policies.



On the *Policy & Objects* pane, go to *Tools > Display Options*, and then select the *Explicit Proxy Policy* checkbox in the *Policy* section to display this option.

To create a new proxy policy:

1. Go to *Policy & Objects > Policy Packages*.
2. In the tree menu for the policy package in which you will be creating the new policy, select *Explicit Proxy Policy*.
3. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.

4. Enter the following information, then click *OK* to create the policy:

Explicit Proxy Type	Select the explicit proxy type: <i>Explicit Web</i> , <i>Transparent Web</i> , <i>FTP</i> , or <i>WAN Opt</i> .
Incoming Interface	Select incoming interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. This option is only available when the proxy type is set to <i>Transparent Web</i> .
Outgoing Interface	Select outgoing interfaces.
Source	Select source addresses.

Destination	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups from the object selector pane.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>Deny</i> , <i>Accept</i> , or <i>Redirect</i> . <i>Redirect</i> is only available when the proxy type is set to <i>Explicit Web</i> , or <i>Transparent Web</i> .
Log Traffic	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • <i>No Log</i> • <i>Log Security Events</i> • <i>Log All Sessions</i> <p>When <i>Log All Sessions</i> is selected, you can select to generate logs when the session starts.</p> <p>This option is available when the <i>Action</i> is <i>Accept</i>.</p>
Log Violation Traffic	<p>Select to log violation traffic.</p> <p>This option is available when the <i>Action</i> is <i>Deny</i>.</p>
Disclaimer Options	<p>Set the Display Disclaimer: <i>Disable</i>, <i>By Domain</i>, <i>By Policy</i>, or <i>By User</i>. Optionally, select a custom message in the <i>Customize Messages</i> drop-down if not disabled.</p> <p>These options are available when the <i>Action</i> is <i>Accept</i>.</p>
Security Profiles	<p>Select to add security profiles or profile groups.</p> <p>The following profile types can be added:</p> <ul style="list-style-type: none"> • Antivirus Profile • Web Filter Profile - not available when the proxy type is set to <i>FTP</i> • Application Control - not available when the proxy type is set to <i>FTP</i> • CASI - not available when the proxy type is set to <i>FTP</i> • IPS Profile - not available when the proxy type is set to <i>FTP</i> • DLP Sensor • ICAP - not available when the proxy type is set to <i>FTP</i> • Web Application Firewall - not available when the proxy type is set to <i>FTP</i> • Proxy Options • SSL/SSH Inspection • Profile Group (available when <i>Use Security Profile Group</i> is selected) <p>This option is available when the <i>Action</i> is <i>Accept</i>.</p>
Redirect URL	<p>Enter the redirect URL.</p> <p>This option is only available when the <i>Action</i> is <i>Redirect</i>.</p>
Web Proxy Forwarding Server	<p>Select a web proxy forwarding server from the dropdown list.</p> <p>This option is not available when the proxy type is set to <i>FTP</i>.</p>

Description	Add a description of the policy, such as its purpose, or the changes that have been made to it.
Advanced Options	Configure advanced options, see Advanced options below. For more information on advanced option, see the <i>FortiOS CLI Reference</i> .

Advanced options

Option	Description	Default
dstaddr-negate	Enable or disable negated destination address match.	disable
global-label	Enter a global label.	none
http-tunnel-auth	Enable or disable	
internet-service-negate	Enable or disable negated internet service.	disable
label	Enter a label	none
poolname	Select a firewall IP pool from the dropdown list.	none
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers.	disable
service-negate	Enable or disable negated service match.	disable
srcaddr-negate	Enable or disable negated source address match.	disable
tags	Applied object tags.	none
transparent	Use IP address of client to connect to server.	disable
webcache	Enable or disable web cache.	disable
webcache-https	Enable or disable web cache for HTTPS.	disable
webproxy-profile	Select a webproxy profile from the dropdown list.	none

Central SNAT

The Central SNAT (Secure NAT) table enables you to define and control (with more granularity) the address translation performed by the FortiGate unit. With the NAT table, you can define the rules which dictate the source address or address group, and which IP pool the destination address uses.

While similar in functionality to IP pools, where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to guarantee the source port number is unchanged. If no fixed port is defined, the port translation is randomly chosen by the FortiGate unit. With the central NAT table, you have full control over both the IP address and port translation.

The FortiGate unit reads the NAT rules in a top-down methodology, until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. The NAT policies can be rearranged within the policy list as well. NAT policies are applied to network traffic after a security policy.

The Central SNAT table allows you to create, edit, delete, and clone central SNAT entries.



Central SNAT does not support *Section View*.



Central NAT must be enabled, or *NGFW Mode* must be set to *Policy-based*, when creating or editing the policy package for this option to be available in the tree menu. See [Create new policy packages on page 217](#).

To create a new central SNAT entry:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central SNAT*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Central SNAT* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

Incoming Interface	Click the field then select interfaces from the <i>Object Selector</i> frame, or drag and drop the address from the object pane. Select the remove icon to remove values.
Outgoing Interface	Select outgoing interfaces.
Source Address	Select source addresses.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
NAT	Select to enable NAT.
IP Pool Configuration	Select either <i>Use Outgoing Interface Address</i> , or <i>Use Dynamic IP Pool</i> . If using a dynamic IP pool, select the pool from the <i>Object Selector</i> frame. This option is only available when <i>NAT</i> is selected.
Protocol	Select the protocol: <i>ANY</i> , <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>Specify</i> . If <i>Specify</i> is selected, specify the protocol number. This option is only available when <i>NAT</i> is selected.
Advanced Options	Enable or disable <i>nat</i> .

Central DNAT

The FortiGate unit checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. DNAT is typically applied to traffic from the Internet that is going to be directed to a server on a network behind the FortiGate device. DNAT means the actual address of the internal network is hidden from the Internet. This step determines whether a route to the destination address actually exists.

DNAT must take place before routing so that the unit can route packets to the correct destination.

DNAT policies can be created, or imported from Virtual IP (VIP) objects. Virtual servers can also be imported from ADOM objects to DNAT policies. DNAT policies are automatically added to the VIP object table (*Object Configurations > Firewall Objects > Virtual IPs*) when they are created.

VIPs can be edited from either the DNAT or VIP object tables by double-clicking on the VIP, right-clicking on the VIP and selected *Edit*, or selecting the VIP and clicking *Edit* in the toolbar. The network type cannot be changed. DNAT policies can also be copied, pasted, cloned, and moved from the right-click or *Edit* menus.

Deleting a DNAT policy does not delete the corresponding VIP object, and a VIP object cannot be deleted if it is in the DNAT table.

DNAT policies support overlapping IP address ranges; VIPs do not. DNAT policies do not support VIP groups.



Central DNAT does not support *Section View*.



Central NAT must be enabled when creating or editing the policy package for this option to be available in the tree menu. See [Create new policy packages on page 217](#).

To create a new central DNAT entry:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central DNAT*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Virtual IP* pane opens.
5. Configure the following settings, then click *OK* to create the VIP:

Name	Enter a unique name for the DNAT.
Comments	Optionally, enter comments about the DNAT, such as its purpose, or the changes that have been made to it.
Color	Select a color.
Interface	Select an interface.
Network	
Type	Select the network type: <i>Static NAT</i> , <i>DNS Translation</i> , or <i>FQDN</i> .
External IP Address/Range	Enter the start and end external IP addresses in the fields. If there is only one address, enter it in both fields. This option is not available when the network type is <i>FQDN</i> .

Mapped IP Address/Range	Enter the mapped IP address. This option is not available when the network type is <i>FQDN</i> .
External IP Address	Enter the external IP address. This option is only available when the network type is <i>FQDN</i> .
Mapped Address	Select the mapped address. This option is only available when the network type is <i>FQDN</i> .
Source Interface Filter	Select a source interface filter.
Source Interface Filter	Select a source interface filter.
Optional Filters	Enable or disable optional filters.
Source Address	Add source IP, range, or subnet filters. Multiple filters can be added using the <i>Add</i> icon.
Services	Enable and add services.
Port Forwarding	Enable or disable port forwarding.
Protocol	Select the protocol: <i>TCP</i> , <i>UDP</i> , <i>SCTP</i> , or <i>ICMP</i> .
External Service Port	Enter the external service port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
Map to Port	Enter the map to port. This option is not available when <i>Protocol</i> is <i>ICMP</i> .
Enable ARP Reply	Select to enable ARP reply.
Advanced Options	Configure advanced options, see Advanced options . For more information on advanced option, see the <i>FortiOS CLI Reference</i> .
Per-Device Mapping	If multiple imported VIP objects have the same name but different details, the object type will become Dynamic Virtual IP, and the per-device mappings will be listed here. Mappings can also be manually added, edited, and deleted as needed.

To import VIPs from the Virtual IP object table:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Central DNAT*.
4. Click *Import* in the toolbar. The *Import* dialog box will open.
5. Select the VIP object or objects that need to be imported. If necessary, use the search box to locate specific objects.
6. Click *OK* to import the VIPs to the *Central DNAT* table.

Advanced options

Option	Description	Default
dns-mapping-ttl	Enter time-to-live for DNS response, from 0 to 604 800. 0 means use the DNS server's response time.	0
extaddr	Select an address.	None
gratuitous-arp-interval	Set the time interval between sending of gratuitous ARP packets by a virtual IP. 0 disables this feature.	0
http-cookie-age	Set how long the browser caches cooking, from 0 to 525600 seconds.	60
http-cookie-domain	Enter the domain name to restrict the cookie to.	none
http-cookie-domain-from-host	If enabled, when the unit adds a SetCookie to the HTTP(S) response, the Domain attribute in the SetCookie is set to the value of the Host: header, if there is one.	disable
http-cookie-generation	The exact value of the generation is not important, only that it is different from any generation that has already been used.	0
http-cookie-path	Limit the cookies to a particular path.	none
http-cookie-share	Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain. Disable to make sure that a cookie generated for a virtual server cannot be used by other virtual servers.	same-ip
http-ip-header-name	Enter a name for the custom HTTP header that the original client IP address is added to.	none
https-cookie-secure	Enable or disable using secure cookies for HTTPS sessions.	disable
id	Custom defined ID.	0
max-embryonic-connections	The maximum number of partially established SSL or HTTP connections, from 0 to 100000.	1000
nat-source-vip	Enable to prevent unintended servers from using a virtual IP. Disable to use the actual IP address of the server (or the destination interface if using NAT) as the source address of connections from the server that pass through the device.	disable
outlook-web-access	If enabled, the <code>Front-End-Https: on</code> header is inserted into the HTTP headers, and added to all HTTP requests.	disable

Option	Description	Default
ssl-algorithm	Set the permitted encryption algorithms for SSL sessions according to encryption strength: <ul style="list-style-type: none"> high: permit only high encryption algorithms: AES or 3DES. medium: permit high or medium (RC4) algorithms. low: permit high, medium, or low (DES) algorithms. custom: only allow some preselected cipher suites to be used. 	high
ssl-client-fallback	Enable to prevent Downgrade Attacks on client connections.	enable
ssl-client-renegotiation	Select the SSL secure renegotiation policy. <ul style="list-style-type: none"> allow: allow, but do not require secure renegotiation. deny: do not allow renegotiation. secure: require secure renegotiation. 	allow
ssl-client-session-state-max	The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the unit, from 0 to 100000.	1000
ssl-client-session-state-timeout	The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the unit, from 1 to 14400.	30
ssl-client-session-state-type	The method to use to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate. <ul style="list-style-type: none"> both: expire SSL session states when either <code>ssl-client-session-state-max</code> or <code>ssl-client-session-state-timeout</code> is exceeded, regardless of which occurs first. count: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded. disable: expire all SSL session states. time: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded. 	both
ssl-dh-bits	The number of bits used in the Diffie-Hellman exchange for RSA encryption of the SSL connection: 768, 1024, 1536, 2048, 3072, or 4096.	2048
ssl-hpkip	Enable or disable including HPKP header in response.	disable
ssl-hpkip-age	The number of seconds that the client should honor the HPKP setting (60 - 157680000).	5184000
ssl-hpkip-backup	Certificate to generate the backup HPKP pin from (size = 35, datasource(s) = vpn.certificate.local.name, vpn.certificate.ca.name).	None
ssl-hpkip-include-subdomains	Enable or disable indicating that the HPKP header applies to all subdomains.	disable
ssl-hpkip-primary	Certificate to generate the primary HPKP pin from (size = 35, datasource(s) = vpn.certificate.local.name, vpn.certificate.ca.name).	None
ssl-hpkip-report-uri	URL to report HPKP violations to (size = 255).	

Option	Description	Default
ssl-hsts	Enable or disable including HSTS header in response.	disable
ssl-hsts-age	The number of seconds that the client should honour the HSTS setting (60 - 157680000).	5184000
ssl-hsts-include-subdomains	Enable or disable indicating that the HSTS header applies to all subdomains.	disable
ssl-http-location-conversion	Enable to replace http with https in the reply's Location HTTP header field.	disable
ssl-http-match-host	Enable to apply Location conversion to the reply's HTTP header only if the host name portion of Location matches the request's Host field or, if the Host field does not exist, the host name portion of the request's URI.	disable
ssl-max-version	The highest version of SSL/TLS to allow in SSL sessions: <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , or <code>tls-1.2</code> .	tls-1.2
ssl-min-version	The lowest version of SSL/TLS to allow in SSL sessions: <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , or <code>tls-1.2</code> .	tls-1.0
ssl-pfs	Select the handling of Perfect Forward Secrecy (PFS) by controlling the cipher suites that can be selected. <ul style="list-style-type: none"> <code>allow</code>: allow use of any cipher suite so PFS may or may not be used depending on the cipher suite selected. <code>deny</code>: allow only non-Diffie-Hellman cipher-suites, so PFS is not applied. <code>require</code>: allow only Diffie-Hellman cipher-suites, so PFS is applied. 	allow
ssl-send-empty-frags	Enable to precede the record with empty fragments to thwart attacks on CBC IV. Disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.	enable
ssl-server-algorithm	Set the permitted encryption algorithms for SSL server sessions according to encryption strength: <ul style="list-style-type: none"> <code>high</code>: permit only high encryption algorithms: AES or 3DES. <code>medium</code>: permit high or medium (RC4) algorithms. <code>low</code>: permit high, medium, or low (DES) algorithms. <code>custom</code>: only allow some preselected cipher suites to be used. 	client
ssl-server-max-version	The highest version of SSL/TLS to allow in SSL server sessions: <code>client</code> , <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , or <code>tls-1.2</code> .	client
ssl-server-min-version	The lowest version of SSL/TLS to allow in SSL server sessions: <code>client</code> , <code>ssl-3.0</code> , <code>tls-1.0</code> , <code>tls-1.1</code> , or <code>tls-1.2</code> .	client
ssl-server-session-state-max	The maximum number of SSL session states to keep for the segment of the SSL connection between the client and the unit, from 0 to 100000.	100

Option	Description	Default
ssl-server-session-state-timeout	The number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the unit, from 1 to 14400.	60
ssl-server-session-state-type	<p>The method to use to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate.</p> <ul style="list-style-type: none"> both: expire SSL session states when either <code>ssl-client-session-state-max</code> or <code>ssl-client-session-state-timeout</code> is exceeded, regardless of which occurs first. count: expire SSL session states when <code>ssl-client-session-state-max</code> is exceeded. disable: expire all SSL session states. time: expire SSL session states when <code>ssl-client-session-state-timeout</code> is exceeded. 	both
weblogic-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebLogic server.	disable
websphere-server	Enable or disable adding an HTTP header to indicate SSL offloading for a WebSphere server.	disable

DoS policy

The *IPv4 DoS Policy* and *IPv6 DoS Policy* panes allow you to create, edit, delete, and clone DoS policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 DoS Policy* and *IPv6 DoS Policy* checkboxes to display these options.

To create a DoS policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *IPv4 DoS Policy* or *IPv6 DoS Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

Incoming Interface	Select the incoming interface from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Source Address	Select the source address.
Destination Address	Select the destination address.
Service	Select the service.

L3 Anomalies

ip_src_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

ip_dst_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

L4 Anomalies

tcp_syn_flood Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 2000.

tcp_port_scan Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 1000.

tcp_src_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

tcp_dst_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

udp_flood Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 2000.

udp_scan Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 2000.

udp_src_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

udp_dst_session Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 5000.

icmp_flood Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 250.

icmp_sweep Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold.
The default threshold is 100.

icmp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 300.
icmp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
sctp_flood	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 2000.
sctp_scan	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 1000.
sctp_src_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
sctp_dst_session	Select to enable the DoS status and logging, select the action to pass, block or proxy, and configure the threshold. The default threshold is 5000.
Advanced Options	Optionally, add a description of the policy, such as its purpose, or the changes that have been made to it.

Interface policy

The *IPv4 Interface Policy* and *IPv6 Interface Policy* panes allow you to create, edit, delete, and clone interface policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Interface Policy* and *IPv6 Interface Policy* check boxes to display these options.

To create a new interface policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *IPv4 Interface Policy* or *IPv6 Interface Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
5. Configure the following settings, then click *OK* to create the policy:

Source

Interface	Select the source zone from the <i>Object Selector</i> frame, or drag and drop the address from the object pane.
Address	Select the source address.
Destination	
Address	Select the destination address.
Service	Select the service.
Log Traffic	Select the traffic to log: <i>No Log</i> , <i>Log Security Events</i> , or <i>Log All Sessions</i> .
AntiVirus Profile	Select to enable antivirus and select the profile from the dropdown list.
Web Filter Profile	Select to enable Web Filter and select the profile from the dropdown list.
Application Control	Select to enable Application Control and select the profile from the dropdown list.
IPS Profile	Select to enable IPS and select the profile from the dropdown list.
Email Filter Profile	Select to enable Email Filter and select the profile from the dropdown list.
DLP Sensor	Select to enable DLP Sensor and select the profile from the dropdown list.
Advanced Options	
comments	Add comments about the policy.
dsri	Enable or disable dsri.
scan-botnet-connections	Enable or disable scanning of connections to Botnet servers.

Multicast policy

Multicasting consists of using a single source to send data to many receivers simultaneously, while conserving bandwidth and reducing network traffic. For information about multicasting, see the *FortiOS Handbook* available in the [Fortinet Document Library](#).



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *Multicast Policy* checkbox to display this option.

To create a new multicast policy:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package, click *Multicast Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be

added to the bottom of the list. The *Create New Policy* pane opens.

5. Configure the following settings, then click *OK* to create the policy:

Incoming Interface	Click in the field and select incoming interfaces from the multicast interface list on the <i>Object Selector</i> frame, or drag and drop the interface from the object pane. If no multicast interfaces are configured, click the <i>Create New Object</i> button to open the <i>Create New Dynamic Multicast Interface</i> window, and then create a new multicast interface.
Outgoing Interface	Click in the field and select outgoing interfaces from the multicast interface list. If no multicast interfaces are configured, one must be created.
Source Address	Click the field and select the source firewall addresses.
Source NAT	Enable source NAT.
Source NAT Address	Enter the source NAT IP address.
Destination Interface	Click the field and select the destination firewall addresses.
Destination NAT	Enter the destination NAT IP address.
Protocol Option	Select a protocol option from the dropdown list: <i>ANY</i> , <i>ICMP</i> , <i>IGMP</i> , <i>TCP</i> , <i>UDP</i> , <i>OSFP</i> , or <i>Others</i> .
Port Range	Set the port range. This option is only available when <i>Protocol Option</i> is <i>TCP</i> or <i>UDP</i> .
Protocol Number	Enter the protocol number, from 1 to 256. This option is only available when <i>Protocol Option</i> is <i>Others</i> .
Log Traffic	Select to log traffic.
Advanced Options	Enable or disable <i>auto-asic-offload</i> , and enter the <i>id</i> number.

Local in policy

The section describes how to create new IPv4 and IPv6 Local In policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *IPv4 Local In Policy* and *IPv6 Local In Policy* checkboxes to display these options.

To create a new Local In policy:

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Local In Policy* or *IPv6 Local In Policy*.

- Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
- Enter the following information, then click *OK* to create the policy:

Interface	Click the field then select an interface from the object selector frame, or drag and drop the interface from the object pane.
Source Address	Select source addresses.
Destination Address	Select destination addresses, address groups, virtual IPs, and virtual IP groups.
Service	Select services and service groups.
Schedule	Select schedules, one time or recurring, and schedule groups.
Action	Select an action for the policy to take: <i>ACCEPT</i> or <i>DENY</i> .
HA Management Interface Only	Select to enable. This option is only available for IPv4 policies.

Traffic shaping policy

The section describes how to create new traffic shaping policies.



On the *Policy & Objects* pane, from the *Tools* menu, select *Display Options*, and then select the *Traffic Shaping Policy* checkbox to display this option.

To create a traffic shaping policy:

- Ensure that you are in the correct ADOM.
- Go to *Policy & Objects > Policy Packages*.
- In the tree menu for the policy package in which you will be creating the new policy, select *Traffic Shaping Policy*. If you are in the Global Database ADOM, select *Traffic Shaping Header Policy* or *Traffic Shaping Footer Policy*.
- Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list. The *Create New Policy* pane opens.
- Enter the following information, then click *OK* to create the policy:

IP Version	Select the IP address version: <i>IPv4</i> or <i>IPv6</i> .
Matching Criteria	
Source	Select sources from the object selector pane.
Destination	Select destinations.
Service	Select services.

Application Category	Select application categories.
Application	Select applications.
URL Category	Select URL categories.
Users	Select users.
User Groups	Select user groups.
Apply Shaper	
Outgoing Interface	Select outgoing interfaces.
Traffic Shaping	Select traffic shapers.
Reverse Traffic Shaping	Select traffic shapers.
Per-IP Traffic Shaping	Select per IP traffic shapers.
Advanced Options	Set the schedule (default = None).

Managing objects and dynamic objects

All objects within an ADOM are managed by a single database unique to that ADOM. Objects inside that database can include items such as addresses, services, intrusion protection definitions, antivirus signatures, web filtering profiles, etc.

Many objects now include the option to enable dynamic mapping. You can create new dynamic maps. When this feature is enabled, a table is displayed which lists the dynamic mapping information. You can also choose to add the object to groups, when available, and add tags.

When making changes to an object within the object database, changes are reflected immediately within the policy table in the GUI; no copying to the database is required. If partial install is enabled, the edited object can be pushed to all the devices that currently use it.

Dynamic objects are used to map a single logical object to a unique definition per device. Addresses, interfaces, virtual IPs, and an IP pool can all be addressed dynamically.



Not all policy and object options are enabled by default. See [Display options on page 216](#).

Objects and dynamic objects are managed in the *Policy & Objects > Object Configurations* pane (on the bottom half of the screen when dual pane is enabled). The available objects vary, depending on the specific ADOM selected.

Objects are used to define policies, and policies are assembled into policy packages that you can install on devices.

Policy packages are managed in the *Policy & Objects > Policy Packages* pane (on the top half of the screen when dual pane is enabled). When you view a policy in a policy package, you edit the policy by dragging objects from other columns, policies, or the object selector frame and dropping the objects in cells in the policy. For more information see [Drag and drop objects on page 233](#).



On the *Policy & Objects > Object Configuration* pane, you can right-click on an object to find out where the object is used (*Where Used*) or to add the object to a group (*Grouping*).

FortiManager objects are defined either per ADOM or at a global level.



On the *Policy & Objects > Object Configuration* pane, you can right-click on an object to find out where the object is used (*Where Used*) or to add the object to a group (*Grouping*).

Create a new object

Objects can be created as global objects, or for specific ADOMs.

To create a new object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Select the object type that you will be creating. For example, view the firewall addresses by going to *Firewall Objects > Address*.

The firewall address list is displayed in the content pane. The available address or address group lists are selectable on the content pane toolbar.

4. From the *Create New* menu, select the type of address. In this example, *Address* was selected. The *New Address* dialog box opens.

Create New Address

Address Name	<input style="width: 80%;" type="text"/>
Comments	<input style="width: 80%;" type="text"/>
Type	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between;"> IP/Netmask ▼ </div>
IP/Netmask	<input style="width: 80%;" type="text" value="0.0.0.0/0.0.0.0"/>
Interface	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between;"> any ▼ </div>
Static Route Configuration	<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #007bff; border: 1px solid #007bff; margin-right: 5px;"></div> ON </div>
Advanced Options >	
Per-Device Mapping	<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #6c757d; border: 1px solid #6c757d; margin-right: 5px;"></div> OFF </div>

OK

Cancel



In 5.2.0 or later, you can select to add the object to groups and enable dynamic mapping. These options are not available for all objects.

5. Enter the required information, then click *OK* to create the new object.

Map a dynamic object

The devices and VDOMs to which a global object is mapped can also be viewed from the object list. In 5.2 or later, you can add an object to groups and enable dynamic mapping. These options are not available for all objects.

When the *Dynamic Mapping* option is available, select *Create New* to configure the dynamic mapping.

To configure a dynamic mapping via a CLI script, the configuration for the mapping must be defined in the dynamic object under the *config dynamic_mapping* sub-tree. The CLI script must be run on a policy package instead of the device database. For information on running CLI scripts, see [Scripts on page 159](#)

Examples:

Example 1: Dynamic VIP

```
config firewall vip
  edit "vip1"
  ...
  config dynamic_mapping
    edit "FW60CA3911000089"-"root"
      set extintf "any"
      set extip 172.18.26.100
      set mappedip 192.168.3.100
      set arp-reply disable
    next
  end
end
```

Example 2: Dynamic Address

```
config firewall address
  edit "address1"
  ...
  config dynamic_mapping
    edit "FW60CA3911000089"-"root"
      set subnet 192.168.4.0 255.255.255.0
    next
  end
end
```

Example 3: Dynamic Interface

```
config dynamic interface
...
  config dynamic_mapping
```

```

edit "FW60CA3911000089"-"root"
    set local-intf internal
    set intrazone-deny disable
next
end
end

```

Modify an existing Interface-Zone Mapping

Interfaces mapped to a zone locally on FortiGate devices are not visible in Device Manager on FortiManager. It is recommended to create objects in FortiManager instead of creating it on FortiGate devices locally. If an interface is already mapped to a zone in FortiGate, it must be unmapped first. A zone must be created in FortiManager, added to a policy and installed to FortiGate. For convenience and ease of use, it is better to manage Object Configuration and Interface Mapping from FortiManager.

If an Interface is mapped to a Zone in FortiGate:

1. Logon to the FortiGate device.
2. Delete the Interface/Zone mapping from *Interfaces* > *[Interface_Name]* > *Delete*.
3. Logon to FortiManager.
4. Go to *Policy & Objects* > *Object Configurations*.
5. Click *Create New* > *Zone*. Configure the settings and create a zone named *Zone_One*. Enable Per-Device Mapping and select the *Mapped Device* and *Device Interface*.
6. Go to *Policy & Objects* > *Policy Packages*. Select *Create New* from the *Policy Package* drop-down.
7. In the *Create New Policy Package* dialog, specify the name as *New_Policy_Package*.
8. Click the *New_Policy_Package* and click *Create New*. Specify the name as *New_IPv4_Policy* and include *Zone_One* in the policy.
9. Click *New_IPv4_Policy* and click *Installation Target*. Assign the FortiGate device to this policy.
10. Right-click *New Policy Package* and select *Install Wizard*. Select *Install Policy Package & Device Settings* and select the *New Policy Package* from the drop-down. Complete the installation as per the Install Wizard. *Zone_One* is now available on the FortiGate device and mapped as specified in step 5.



A zone is installed to FortiGate devices only if it is created, mapped to an interface, included in the Policy Package, assigned to a device, and installed using the Install Wizard in FortiManager.

An interface cannot be reused if it is already mapped to a zone. To reuse an interface, first unmap it from a zone in *Object Configurations*, and then reinstall on the FortiGate device. After a Virtual IP is created, it must be mapped to interfaces. If per-device mapping is used, the mapping will be visible immediately in *Device Manager* > *[Device_Name]* > *Interface* listing for the particular device.

Map a dynamic device group

When you create and edit a device group, you can choose whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group.

To create a dynamic device group:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations > User & Device > Customer Devices & Groups*.
3. From the *Create New* menu, select *Device Group*.
4. Complete the following options, then click *OK*.

Group Name	Type a name for the device group.
Managed on ADOM	Specify whether to use the FortiManager ADOM or the FortiGate device to manage members for the device group. When you select the <i>Managed on ADOM</i> checkbox, the FortiManager ADOM manages members for the object, and you must specify members for the object. When you clear the <i>Manage on ADOM</i> checkbox, the FortiGate device manages members for the object, and you must specify members by using FortiGate, not FortiManager.
Members	Select members for the device group.
Comments	(Optional) Type a comment.
Per-Device Mapping	Select to enable dynamic mapping for a device.

Remove an object

To remove an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Select the object, and click *Delete*.

You can delete the object, even when the object is used by a policy. After you delete the object, the policy is updated to replace the IP address for the object with the word *None*.

Edit an object

After editing an object in the object database, the changes are immediately reflected within the policy table in the GUI; no copying to the database is required. If partial install is enabled, the edited object can be manually pushed to all devices currently using that object, see [Push to device on page 266](#).

To edit an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. Select an object, then click *Edit*.
5. Edit the information as required, and click *OK*.



Objects can also be edited directly from the policy list and *Object Selector* frame by right-clicking on the object and selecting *Edit*.

Push to device

An object can be manually pushed to all devices that are currently using that object. Partial install must be enabled in the CLI for this option to be available.

To enable partial install:

In the *CLI Console* widget, or any terminal emulation software, enter the following commands:

```
config system global
    set partial-install enable
end
```

To push an object or objects to devices:

1. In the *Object Configurations* pane, locate the objects to push.
2. Select the objects then click *More > Push To Device* in the toolbar, or right-click on the objects and select *Push To Device*.

The *Push To Device* dialog box opens, and the selected object or objects are pushed to all of the devices that currently use them.



After an object is pushed to a device, policy packages will be flagged as modified until the next time the packages are installed.



Global database objects cannot be pushed to devices.

Clone an object

If a new object that you are creating is similar to a previously created object, the new object can be created by cloning the previous object.

To clone an object:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.

4. Right-click an object, and select *Clone*. The *Clone* pane is displayed.
5. Adjust the information as required, and click *OK* to create the new object.

Search objects

The search objects tool allows you to search objects based on keywords.

To dynamically search objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. In the tree menu, select an object type. The content pane displays the objects for the object type.
4. In the search box on the right side lower content frame toolbar type a search keyword. The results of the search are updated as you type and displayed in the object list.

Find unused objects

You can find unused objects.

To find unused objects:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects*.
3. From the *Tools* menu, select *Unused Objects*. The *Unused Objects* dialog box is displayed.
4. When you are done, click *Close*.

Find and merge duplicate objects

Duplicate objects have the same definition, but different names. You can find duplicate objects and review them. You then have the option to merge duplicate objects into one object.

To find duplicate objects:

1. Go to *Policy & Objects*.
2. From the *Tools* menu, select *Find Duplicate Objects*. The *Duplicate Objects* dialog box is displayed.
3. Review the groups of duplicate objects.
4. Click *Merge* to merge a group of duplicate objects into one object.
5. When you are done, click *Close*.

CLI-Only objects

FortiManager 5.2.0 or later adds the ability to configure objects that are available only via the FortiOS command line interface, as well as settings that are not available in the FortiManager GUI.

FortiToken configuration example

To configure FortiToken objects for FortiToken management:

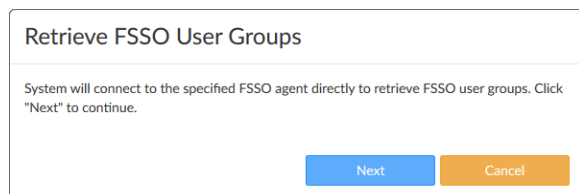
1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*.
3. Go to *User & Device > FortiTokens*.
4. Click *Create New*.
5. Type the serial number or serial numbers of the FortiToken unit or units and click *OK*. Up to ten serial numbers can be entered.
6. Go to *User & Device > User Definition* to create a new user.
7. When creating the new user, select *FortiToken*, and then select the FortiToken from the dropdown menu.
8. Go to *User & Device > User Groups*, create a new user group, and add the previously created user to this group.
9. Install a policy package to the FortiGate, as described in [Install a policy package on page 221](#).
10. On the FortiGate, select *User > FortiToken*. Select one of the newly created FortiTokens, then select *OK* to activate the FortiToken unit.

FSSO user groups

FSSO user groups can be retrieved directly from FSSO, from an LDAP server, via a remote FortiGate device, or by polling the active directory server. Groups can also be entered manually.

To get groups from FSSO:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list.
4. Enter a unique name for the agent in the *Name* field.
5. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
6. Select *From FSSO Agents* in the *Select FSSO Groups* field.
7. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* dialog box will open.



8. Click *Next*. The groups are retrieved from the FSSO.
9. Click *OK*. The groups can now be used in user groups, which can then be used in policies.

To get groups from an LDAP server:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list.

4. Enter a unique name for the agent in the *Name* field.
5. Select an LDAP server from the dropdown list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
6. Select groups from the *Groups* tab, then select *Add Selected* to add the groups.
You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select *OK*.

To get groups via a remote FortiGate:



The FortiGate device configuration must be synchronized or retrieving the FSSO user groups will fail. See [Checking device configuration status on page 145](#).

1. Go to *Policy & Objects > Object Configurations*, and select *User & Device > Single Sign-On*.
2. Click *Create New > Fortinet Single Sign-On Agent* from the dropdown list. The *Create New Fortinet Single Sign-On Agent* window opens.

3. Enter a unique name for the agent in the *Name* field.
4. Enter the IP address or name, password, and port number of the FSSO servers in the FSSO Agent field. Add and remove servers as needed by clicking the *Add* and *Remove* icons at the end of the rows.
5. Select *Via FortiGate* in the *Select FSSO Groups* field.
6. Click *Apply & Refresh*. The *Retrieve FSSO User Groups* wizard will open.

7. Click *Next* to proceed with the wizard.
8. Select the device that the FSSO groups will be imported from. This device must be registered to the FortiManager, its configuration must be synchronized, and it must be able to communicate with the FSSO server.
9. Click *Next*. The FSSO agent is installed on the FortiGate, the FortiGate retrieves the groups, and then the groups are imported to the FortiManager.

Retrieve FSSO User Groups

Group Imported Successfully

100%

- ✓ Installing FSSO Agent to FortiGate
- ✓ Waiting for FortiGate to Sync with FSSO
- ✓ Retrieving FSSO Groups to Device Manager
- ✓ Importing FSSO Groups

Finish Cancel

10. After the groups have been imported, click **Finish**. The imported groups will be listed in the *User Groups* field.

Create New Fortinet Single Sign-On Agent

Name: fss01

FSSO Agent

IP/Name	Password	Port	
10.222.788.878	••••••••	8000	+ 🗑
	••••••••	8000	+ 🗑

Select FSSO Groups: ☐ From FSSO Agents ☒ Via FortiGate

User Groups:

- CN=a'test,DC=FSSOtest,DC=com
- CN=qa01.fmg,CN=Users,DC=FSSOtest,DC=com
- CN=qa03,CN=Users,DC=FSSOtest,DC=com
- CN=qa04,CN=Users,DC=FSSOtest,DC=com
- OU=EQUIPE,DC=FSSOtest,DC=com

LDAP Server:

Per-Device Mapping: ☐ OFF

Advanced Options >

Apply & Refresh OK Cancel

11. Click **OK**. The groups can now be used in user groups, which can then be used in policies.



You must rerun the wizard to update the group list. It is not automatically updated.

To get groups from AD:

1. Ensure you are in the correct ADOM.
2. Go to *Policy & Objects > Object Configurations*. and select *User & Device > Single Sign-On*.
3. Click *Create New > Poll Active Directory Server* from the dropdown list.
4. Configure the server name, local user, password, and polling.
5. Select an LDAP server from the dropdown list. LDAP Servers can be added and configured from *User & Device > LDAP Servers*.
6. Select groups from the *Groups* tab, then select *Add Selected* to add the groups.
You can also select *Manually Specify* in the *Select LDAP Groups* field, and then manually enter the group names.
7. Select **OK**.

Interface mapping

After creating an interface on the FortiManager, an interface mapping must be created so that the new interface can be used when creating policies. To do this, create a new dynamic interface with per-device mapping.

To create a new dynamic interface with per-device mapping:

1. Ensure you are in the correct ADOM.
 2. Go to *Policy & Objects > Object Configurations*.
 3. Go to *Zone/Interface > Interface* and click *Create New > Dynamic interface*.
 4. Enter a name and description for the dynamic interface.
 5. Turn on *Per-Device Mapping*.
 6. Click *Add*. The *Per-Device Mapping* dialog box opens.
 7. Select the device or VDOM in the *Mapped Device* field, select the interface in the *Device Interface* field, then click *OK*.
 8. Click *OK* to create the new dynamic interface object.
- The mapped interface can now be used when creating policies.

VIP mapping

Normally, Virtual IP (VIP) objects map to a single interface, or *ANY*, just as with FortiOS. In the special case where the interface that the VIP is bound to belongs to a zone, FortiManager handles importing and installing the object in a unique way.

When importing a policy package, the VIP is bound to the zone instead of the interface. If per-device mapping is enabled for the VIP, FortiManager automatically adds dynamic mapping for that device that maps the VIP to the specific interface. To use the VIP on another FortiGate, you can add an interface mapping entry for the other FortiGate. The zone acts as filter, limiting the interfaces that can be selected. That is, you can only select an external interface that is a member of the selected zone.

FortiManager binds the VIP to a zone because it needs to know which policies the VIP could be applied to. FortiGate devices use different logic because they already know the zone membership.

In FortiOS, VIPs can only be bound to an interface, and not a zone. Consequently, if there is no matching per-device mapping, FortiManager will convert the binding to *ANY* when installing configuration changes to FortiGate. Depending on the circumstance, this can be avoided by:

- Leaving per-device mapping enabled on the VIP at the ADOM, and letting FortiManager add the required per-device mappings.
- If you are configuring FortiManager to start using the VIP on other FortiGates, adding the per-device mappings manually.

Fortinet SDN Connector

FortiManager supports Fortinet SDN Connector and the following products:

- VMware NSX—see [Fortinet SDN Connector and VMware NSX on page 272](#)
- Cisco Application Centric Infrastructure (ACI)—see [Fortinet SDN Connector and ACI on page 272](#)

Fortinet SDN Connector and VMware NSX

With FortiManager and Fortinet SDN Connector, you can import security groups from VMware NSX to automatically create objects that you can use in an IPv4 virtual wire pair policy. When you install the policy to FortiGate VMX Service Manager, the information is used to communicate with VMware NSX and to dynamically populate the objects with IP addresses.

Requirements:

- FortiManager 5.6 ADOM
- FortiGate VMX Service Manager is managed by FortiManager
- The managed FortiGate VMX Service Manager is configured to work with VMware NSX



You cannot import a policy package for Fortinet SDN Connector from FortiGate VMX Service Manager to FortiManager.

- IPv4 virtual wire pair policy
FortiGate VMX Service Manager requires the use of an IPv4 virtual wire pair policy.

Following is a high-level overview of the configuration procedure:

1. In FortiManager, ensure that you are using a 5.6 ADOM.
2. Create an SDN Connector object for VMware NSX. See [Configuring SDN Connector objects on page 273](#).
3. Import security groups from VMware NSX to the SDN Connector object. See [Importing security groups to SDN Connector objects on page 274](#).
The security groups are imported and converted to firewall address objects. The objects do not yet include IP addresses. The objects are displayed on the *Firewall Objects > Addresses* pane.
4. Create a virtual wire pair. See [Configuring virtual wire pairs on page 275](#).
5. In the policy package in which you will be creating the new policy, create an IPv4 virtual wire pair policy, select the virtual wire pair, and add the firewall address objects for the VMware NSX. See [Virtual wire pair policy on page 242](#).
6. Install the policy package to FortiGate VMX Service Manager. See [Install a policy package on page 221](#).
The FortiGate VMX Service Manager communicates with VMware NSX to dynamically populate the firewall address objects with IP addresses.

If the security groups change in VMware NSX after you import them to FortiManager, you must import the security groups again.

Fortinet SDN Connector and ACI

With FortiManager and Fortinet SDN Connector, you can import security groups from Application Centric Infrastructure (ACI) to automatically create objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information to communicate with ACI and dynamically populate the objects with IP addresses.

Requirements:

- FortiManager 5.6 ADOM
- FortiGate is managed by FortiManager

- The managed FortiGate unit is configured to work with Application Centric Infrastructure (ACI)



You cannot import a policy package for Fortinet SDN Connector from FortiGate to FortiManager.

Following is a high-level overview of the configuration procedure:

1. In FortiManager, ensure that you are using a 5.6 ADOM.
2. Create an SDN Connector object for ACI. See [Configuring SDN Connector objects on page 273](#).
3. Import security groups from ACI to the SDN Connector object. See [Importing security groups to SDN Connector objects on page 274](#).
The security groups are imported and converted to firewall address objects. The objects do not yet include IP addresses. The objects are displayed on the *Firewall Objects > Addresses* pane.
4. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for ACI. See [IP policies on page 237](#).
5. Install the policy package to FortiGate. See [Install a policy package on page 221](#).
FortiGate communicates with ACI to dynamically populate the firewall address objects with IP addresses.

If the security groups change in ACI after you import them to FortiManager, you must import the security groups again.

Configuring SDN Connector objects

You can use FortiManager to create SDN Connector objects for the following products:

- VMware NSX
- Cisco Application Centric Infrastructure (ACI)



You must display the option before you can set it. On the *Policy & Objects > Object Configurations* pane, from the *Tools* menu, select *Display Options*. In the *User & Device* section, select the *SDN Connector* checkbox to display this option.

To create an SDN Connector object:

1. Go to *Policy & Objects > Object Configurations*.
2. Expand *User & Device*, and select *SDN Connector*.
3. In the content pane, click *Create New*.
4. Configure the following options, and then click *OK*:

Name	Type a name for the SDN Connector object.
Type	Specify the type of SDN Connector object. Select one of the following options: <ul style="list-style-type: none">• Application Centric Infrastructure (ACI)• VMware NSX
IP	Type the IP address for the Fortinet SDN Connector.

Port	Identify the port used for the Fortinet SDN Connector. Perform one of the following options: <ul style="list-style-type: none"> Click <i>Use Default</i> to use the default port. Click <i>Specify</i> and type the port number. This option is available when <i>Type</i> is <i>Application Centric Infrastructure (ACI)</i> .
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.
Update Interval (s)	Specify how often in seconds that FortiGate VMX Service Manager should communicate with VMware NSX to update the firewall objects. This option is available when <i>Type</i> is <i>VMware NSX</i> .
Status	Toggle <i>On</i> to enable the SDN Connector object. Toggle <i>OFF</i> to disable the SDN Connector object.
VMX	The <i>VMX</i> options identify settings used by the FortiGate VMX Service Manager to communicate with the REST API for NSX Manager. This option is available when <i>Type</i> is <i>VMware NSX</i> .
	Service Name Type the name of the FortiGate VMX service defined on NSX Manager.
	Image Location Type the location of the FortiGate VMX deployment template used by NSX Manager to deploy the FortiGate VMX service.
REST API	The <i>REST API</i> options specify how the FortiGate VMX Service Manager communicates with the REST API for NSX Manager. This option is available when <i>Type</i> is <i>VMware NSX</i> .
	Port Type the port used by the FortiGate VMX Service Manager to communicate with NSX Manager.
	Interface Select the interface used by the FortiGate VMX Service Manager to communicate with NSX Manager. Choose between <i>Mgmt</i> and <i>Sync</i> .
	Password Type the password that FortiGate VMX Service Manager uses with the REST API to communicate with NSX Manager. Note: This is not the admin password for FortiGate VMX Service Manager.

Importing security groups to SDN Connector objects

After you configure an SDN Connector object, you can import security groups from the Fortinet SDN Connector.

To import security groups to SDN Connector objects:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *User & Device > SDN Connector*.

3. In the content pane, right-click the SDN Connector, and select *Import*.
The *Import SDN Connector* dialog box is displayed.
4. Select the security groups, and click *Import*.
The security groups are imported and converted to firewall address objects that are displayed on the *Firewall Objects > Addresses* pane.

Configuring virtual wire pairs

Before you create an IPv4 virtual wire pair policy, you must create a virtual wire pair.



ADOM version 5.4 or 5.6 are required. Earlier ADOM versions are not supported.

To configure virtual wire pairs:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Zone/Interface > Interface*.
3. In the content pane, click *Create New* and select *Virtual Wire Pair*.
4. Complete the following options, and click *OK*.

Name	Type a name for the virtual wire pair.
Interface Members	Select two interface members.
Wildcard VLAN	<p>Toggle <i>ON</i> to enable wildcard VLANs for the virtual wire pair. When enabled, all VLAN-tagged traffic can pass through the virtual wire pair, if allowed by the virtual wire pair firewall policies.</p> <p>Toggle <i>OFF</i> to disable wildcard VLANs for the virtual wire pair.</p>

ADOM revisions

ADOM revision history allows you to maintain a revision of the policy packages, objects, and VPN console settings in an ADOM. Revisions can be automatically deleted based on given variables, and individual revisions can be locked to prevent them being automatically deleted.

To configure ADOM revisions, go to *Policy & Objects*, and click *ADOM Revisions*.

This page displays the following:

ID	The ADOM revision identifier.
-----------	-------------------------------

Name	The name of the ADOM revision. This field is user-defined when creating the ADOM revision. A green lock icon will be displayed beside the ADOM revision name when you have selected <i>Lock this revision from auto deletion</i> .
Created by	The administrator that created the ADOM revision.
Created Time	The ADOM revision creation date and time.
Comment	Optional comments typed in the <i>Description</i> field when the ADOM revision was created.

The following options are available:

Create New	Select to create a new ADOM revision.
Edit	Right-click on a revision in the table and select <i>Edit</i> in the menu to edit the ADOM revision.
Delete	Right-click on a revision in the table and select <i>Delete</i> in the menu to delete the ADOM revision. When <i>Lock this revision from auto deletion</i> is selected, you are not able to delete the ADOM revision.
Restore	Right-click on a revision in the table and select <i>Restore</i> in the menu to restore the ADOM revision. Restoring a revision will revert policy packages, objects and VPN console to the selected version. Select <i>OK</i> to continue.
More > Lock Revision	Right-click on a revision in the table and select <i>Lock</i> from the <i>More</i> menu to lock this revision from auto deletion.
More > Unlock Revision	Right-click on a revision in the table and select <i>Unlock</i> from the <i>More</i> menu to unlock this revision. When the ADOM revision is in an unlocked state, auto deletion will occur in accordance with your auto deletion settings.
View Revision Diff	Right-click on a revision in the table and select <i>View Revision Diff</i> in the menu. The Summary page will be displayed. This page shows the revision differences between the selected revision and the current database.
Settings	Select to configure the automatic deletion settings for ADOM revisions.
Close	Select to close the <i>ADOM Revision</i> dialog box and return to the <i>Policy & Objects</i> tab.

To create a new ADOM revision:

1. Go to *Policy & Objects*, and click *ADOM Revisions*. The *ADOM Revision* dialog box opens.
2. Click *Create New*. The *Create New Revision* dialog box opens.
3. Type a name for the revisions in the *Name* field.
4. Optionally, type a description of the revision in the *Description* field.
5. To prevent the revision from being automatically deleted, select *Lock this revision from auto deletion*.
6. Click *OK* to create the new ADOM revision.

To edit an ADOM revision:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Edit*. The *Edit Revision* dialog box opens.
3. Edit the revision details as required, then click *OK* to apply your changes.

To delete ADOM revisions:

1. Open the *ADOM Revisions* dialog box.
2. Select a revision, and click *Delete*.
You can select multiple revisions by selecting the checkbox beside each revision.
3. Click *OK* in the confirmation dialog box to delete the selected revision or revisions.

To configure automatic deletion:

1. Open the *ADOM Revisions* dialog box, and click *Settings*.
2. Select *Auto delete revision* to enable to automatic deletion of revisions.
3. Select one of the two available options for automatic deletion of revisions:
4. *Keep last x revisions*: Only keep the entered numbered of revisions, deleting the oldest revision when a new revision is created.
5. *Delete revisions older than x days*: Delete all revisions that are older than the entered number of days.
6. Click *OK* to apply the changes.

To restore a previous ADOM revision:

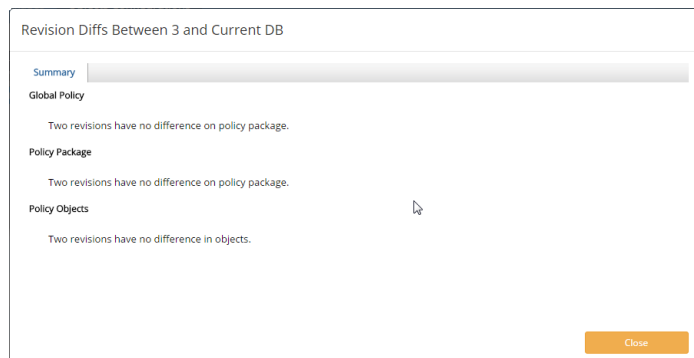
1. Open the *ADOM Revisions* window.
2. Select a revision, and click *Restore*. A confirmation dialog box will appear.
3. Click *OK* to continue.
The *Restore Revision* dialog box opens. Restoring a revision will revert policy packages, objects and VPN console to the selected version.
4. Click *OK* to continue.

To lock or unlock an ADOM revision:

1. Open the *ADOM Revisions* window.
2. Do one of the following:
 - Select a revision, and select *Lock* or *Unlock* from the *More* menu.
 - Edit the revision, and select or clear the *Lock this revision from auto deletion* checkbox in the *Edit ADOM Revision* dialog box.

To view ADOM revision diff:

1. Open the *ADOM Revisions* window.
2. Select a revision, and click *View Revision Diff*. The *Revision Diffs Between* dialog box opens.



This page displays all *Global Policy*, *Policy Package*, and *Policy Objects* changes between the revision selected and the current database.

3. Select *[Details]* to view all details on the changes made to policies and objects.
4. You can select to download this information as a CSV file to your management computer.
5. Click *Close* to return to the *ADOM Revisions* window.

VPN Manager

Use the *VPN Manager* pane to enable and use central VPN management. You can view and configure IPsec VPN and SSL-VPN settings that you can install to one or more devices.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click the mouse on different parts of the navigation panes on the GUI page to access these context menus.

The *VPN Manager* pane includes the following tabs:

IPsec VPN	Displays all of defined IPsec VPN communities and associated devices for the selected ADOM. You can create, monitor, and manage VPN settings. See IPsec VPN Communities on page 282
Monitor	Displays a list of IPsec VPN tunnels, and allows you to bring the tunnels up or down. See Monitoring IPsec VPN tunnels on page 291 .
Map View	Displays a world map showing IPsec VPN tunnels. See Map View on page 291
SSL-VPN	Create, monitor, and manage SSL-VPN settings. You can also create, edit, and delete portal profiles for SSL-VPN settings. See SSL VPN on page 301 .

Overview

When central VPN management is enabled, you can use the *VPN Manager* pane to configure IPsec VPN settings that you can install to one or more devices. The settings are stored as objects in the objects database. You can then select the objects in policies for policy packages on the *Policy & Objects* pane. You install the IPsec VPN settings to one or more devices by installing the policy package to the devices.



You must enable central VPN management to access the settings on the *VPN Manager > IPsec VPN* pane. However, you can access the settings on the *VPN Manager > SSL-VPN* pane without enabling central VPN management. See [Enabling central VPN management on page 280](#).

To create IPsec VPN settings:

1. Enable central VPN management. See [Enabling central VPN management on page 280](#).
2. Create a VPN community, sometimes called a VPN topology. See [Creating IPsec VPN communities on page 282](#).
3. Create a managed gateway. See [Creating managed gateways on page 293](#).

To create SSL-VPN settings:

1. Create custom profiles. See [Creating SSL VPN portal profiles on page 305](#).
Alternately, you can skip this step, and use the default portal profiles.
2. Add an SSL VPN to a device, and select a portal profile. See [Creating SSL VPNs on page 302](#).

To install VPN objects to devices:

1. Plan the VPN security policies. See [VPN security policies on page 300](#).
2. In a policy package, create VPN security policies, and select the VPN settings. See [Creating policies on page 230](#).
3. Edit the installation targets for the policy package to add all of the devices onto which you want to install the policy defined VPN settings. See [Policy package installation targets on page 224](#).
4. Install the policy package to the devices. See [Install a policy package on page 221](#).



VPNs can also be configured directly on a FortiGate. To prevent conflicts, the *preserve* field must be selected in the phase 1 and phase 2 interfaces when creating the VPN. See *The FortiOS Handbook*, in the [Fortinet Document Library](#), for more information.

Enabling central VPN management

You can enable centralized VPN management from the *VPN Manager > IPsec VPN* pane.

You can also enable centralized VPN management by editing an ADOM. When ADOMs are disabled, you can enable centralized VPN management by using the *System Settings > Dashboard* pane.

Regardless of how you enable centralized VPN management, you use the *VPN Manager* module for centralized VPN management.

To enable central VPN management:

1. Go to *VPN Manager > IPsec VPN*.
2. Select *Enable*.
3. Click *OK* in the confirmation dialog box.

To enable central VPN management for an ADOM:

1. Ensure that you are in the correct ADOM.
2. Go to *System Settings > All ADOMs*.
3. Right-click an ADOM, and select *Edit*.
4. In the *Central Management* field, select the *VPN* checkbox.
5. Click *OK*. Centralized VPN management is enabled for the ADOM.

To enable central VPN management when ADOMs are disabled:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, in the *VPN Management Mode* field, select *Change VPN Management Mode*. The *Change VPN Management Mode* dialog box is displayed.
3. Click *OK*.

DDNS support

When Dynamic DNS (DDNS) is enabled on FortiGates, VPN Manager supports DDNS. First VPN Manager searches for the interface IP for IPsec Phase2. If no IP is found, then VPN Manager searches for DDNS.

You can use FortiManager and the CLI-only objects menu to enable DDNS on each FortiGate device. The CLI-only objects menu is available in the Device Manager pane. See [CLI-Only Objects menu on page 131](#).

With the CLI-only objects menu, you can use the `config system ddns` command to enable DDNS on a per-device basis. The selected monitoring interface must be the interface that supports your tunnel, for example:

```
config system ddns
  edit 1
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST1>.fortiddns.com"
    set monitor-interface "port14"
  next
end
```

You can also use the CLI-only objects menu to configure DDNS on multiple FortiGate interfaces. Once configured, you can use FortiManager to view all the DDNS entries, but you cannot edit the entries.

Following is an example of how to configure DDNS on multiple FortiGates by using the CLI-only objects menu:

```
config system ddns
  edit 1
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST1>.fortiddns.com"
    set use-public-ip enable
    set monitor-interface "wan"
  next
  edit 2
    set ddns-server FortiGuardDDNS
    set ddns-domain "<HOST2>.fortiddns.com"
    set use-public-ip disable
    set monitor-interface "wwan"
  next
end
```

Multiple DDNS entries are useful when using SDWAN and multiple broadband links.

IPsec VPN Communities

You can use the *VPN Management > IPsec VPN* pane to create and monitor full-meshed, star, and dial-up IPsec VPN communities. IPsec VPN communities are also sometimes called VPN topologies.

Managing IPsec VPN communities

Go to *VPN Manager > IPsec VPN* to manage IPsec VPN communities.

+ Create New Edit Delete Column Settings <input type="text"/>								
<input type="checkbox"/>	Seq.#	Name	Topology	Gateways	Authentication	Phase 1 Encryption	Phase 2 Encryption	VPN Zone
<input type="checkbox"/>	1	F	Full Mesh	4 Gateways FGT54_1[root] FGT54_1[root] FGT54_2[root] FGT54_2[root]	Pre-shared Key	3des-sha1, 3des-md5	3des-sha1, 3des-md5	✓
<input type="checkbox"/>	2	dual-l	Star		Pre-shared Key	3des-sha1, 3des-md5	3des-sha1, 3des-md5	✓

The following options are available:

VPN Community	Select to create a new VPN community, edit the selected VPN community, or delete the selected VPN community.
Install Wizard	Launch the Install Wizard to install IPsec VPN settings to devices.
Create New	Create a new VPN community. See Creating IPsec VPN communities on page 282
Edit	Edit the selected VPN community. See Editing an IPsec VPN community on page 290 .
Delete	Delete the selected VPN community or communities. See Deleting VPN communities on page 290 .
Column Settings	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
Search	Enter a search term to search the communities list.
Configure Gateways	Go to the gateway list for the community. This option is only available from the right-click menu. See IPsec VPN gateways on page 293 .
Add Managed Gateway	Start the <i>VPN Gateway Setup Wizard</i> . This option is only available from the right-click menu. See Creating managed gateways on page 293 .

Creating IPsec VPN communities

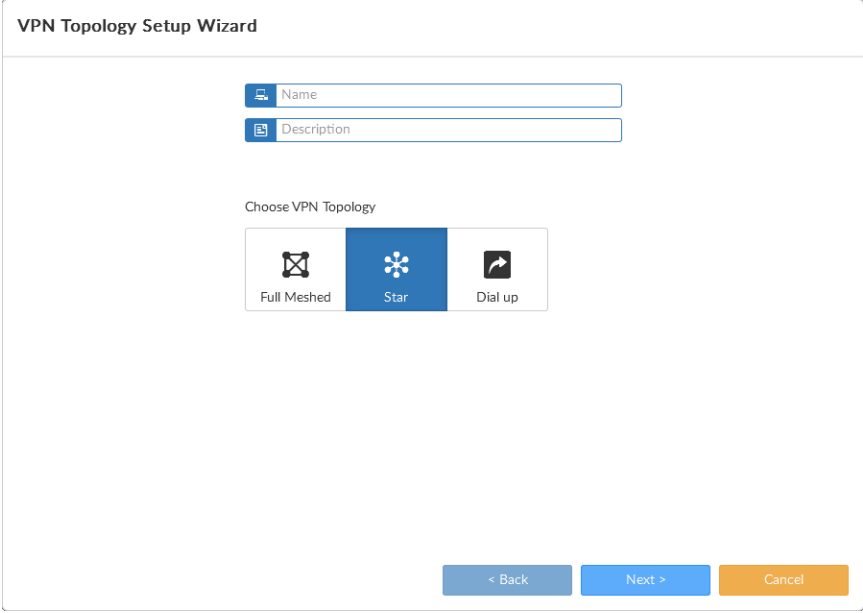
You can create one or more IPsec VPN communities. An IPsec VPN community is also sometimes called a VPN topology. A *VPN Topology Wizard* is available to help you set up topologies.

After you create the IPsec VPN community, you can create the VPN gateway. See [IPsec VPN gateways on page 293](#).

To create a new IPsec VPN community:

1. Go to the *VPN Manager > IPsec VPN* tab.
2. From the *VPN Community* menu, select *Create New*, or click *Create New* in the toolbar.

The *VPN Topology Setup Wizard* is displayed.



The image shows the 'VPN Topology Setup Wizard' dialog box. It has a title bar with the text 'VPN Topology Setup Wizard'. Inside the dialog, there are two input fields: 'Name' and 'Description', each with a small icon to its left. Below these fields is a section titled 'Choose VPN Topology'. This section contains three buttons with icons: 'Full Meshed' (a square with an 'X'), 'Star' (a star icon), and 'Dial up' (a computer monitor icon). The 'Star' button is highlighted with a blue background. At the bottom of the dialog, there are three buttons: '< Back' (disabled), 'Next >' (active), and 'Cancel'.

3. Enter a name for the topology in the *Name* field.
4. Optionally, enter a brief description of the topology in the *Description* field.
5. Choose a topology type: *Full Meshed*, *Star*, or *Dial up*.
 - *Full Meshed*: Each gateway has a tunnel to every other gateway.
 - *Star*: Each gateway has one tunnel to a central hub gateway.
 - *Dial up*: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.

6. Click *Next*.

7. Configure the *Authentication* and *Encryption* information for the topology
 8. Click *Next*.
 9. Configure the *VPN Zone*, *IKE Security Phase 1 Advanced Properties*, *IPsec Security Phase 2 Advanced Properties*, and *Advanced Options*.
 10. Click *Next*.
 11. Review the topology information on the *Summary* page, then click *OK* to create the topology.
- After you have created the VPN topology, you can create managed and external gateways for the topology.



For descriptions of the options in the wizard, see [VPN community settings on page 284](#).

VPN community settings

The following table describes the options available in the *VPN Topology Setup Wizard* and on the *Edit VPN Community* page.

Name	Type a name for the VPN topology.
Description	Type an optional description.
Choose VPN Topology	Choose a topology type. Select one of: <ul style="list-style-type: none"> • <i>Full Meshed</i>: Each gateway has a tunnel to every other gateway. • <i>Star</i>: Each gateway has one tunnel to a central hub gateway. • <i>Dial up</i>: Some gateways, often mobile users, have dynamic IP addresses and contact the gateway to establish a tunnel.

Authentication	<p>Select <i>Certificates</i> or <i>Pre-shared Key</i>.</p> <p>When you select <i>Pre-shared Key</i>, FortiGate implements the Encapsulated Security Payload (ESP) protocol. Internet Key Exchange (IKE) is performed automatically based on pre-shared keys or X.509 digital certificates.</p>
Certificates	<p>If you selected <i>Certificates</i>, select a certificate template. Fortinet provides several default certificate templates. You can also create certificate templates on the <i>Device Manager > Provisioning Templates > Certificate Templates</i> pane.</p>
Pre-shared Key	<p>If you selected <i>Pre-shared Key</i>, select <i>Generate</i> or <i>Specify</i>.</p> <p>When you select <i>Specify</i>, type the pre-shared key that the FortiGate unit will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. You must define the same key at the remote peer or client. The key must contain at least 6 printable characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.</p> <p>Alternatively, you can select to generate a random pre-shared key.</p>
Encryption	<p>Define the IKE Profile. Configure IKE Phase 1 and IKE Phase 2 settings.</p>
IKE Security (Phase 1) Properties	<p>Define the Phase 1 proposal settings.</p>

Encryption Authentication

Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.

You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define.

Select one of the following symmetric-key encryption algorithms:

- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
- AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.
- ARIA128: A 128-bit block size that uses a 128-bit key.
- ARIA192: A 128-bit block size that uses a 19-bit key.
- ARIA256: A 128-bit block size that uses a 256-bit key.
- SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.

Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:

- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.
- SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest.
- SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.
- SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.

To specify a third combination, use the Add button beside the fields for the second combination.

IPsec Security (Phase 2) Properties

Define the Phase 2 proposal settings.

When you define phase 2 parameters, you can choose any set of phase 1 parameters to set up a secure connection for the tunnel and authenticate the remote peer. Auto Key configuration applies to both tunnel-mode and interface-mode VPNs.

**Encryption
Authentication**

Select the encryption and authentication algorithms used to generate keys for protecting negotiations and add encryption and authentication algorithms as required.

You need to select a minimum of one and a maximum of three combinations. The remote peer or client must be configured to use at least one of the proposals that you define.

It is invalid to set both Encryption and Authentication to NULL.

Select one of the following symmetric-key encryption algorithms:

- NULL: Do not use an encryption algorithm.
- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
- AES128: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 128-bit key.
- AES192: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 192-bit key.
- AES256: A 128-bit block Cipher Block Chaining (CBC) algorithm that uses a 256-bit key.
- ARIA128: A 128-bit block size that uses a 128-bit key.
- ARIA192: A 128-bit block size that uses a 19-bit key.
- ARIA256: A 128-bit block size that uses a 256-bit key.
- SEED: A 16-round Feistel network with 128-bit blocks and a 128-bit key.

Select either of the following authentication message digests to check the authenticity of messages during phase 1 negotiations:

- NULL: Do not use a message digest.
- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA1: Secure Hash Algorithm 1, which produces a 160-bit message digest.
- SHA256: Secure Hash Algorithm 2, which produces a 256-bit message digest.
- SHA384: Secure Hash Algorithm 3, which produces a 384-bit message digest.
- SHA512: Secure Hash Algorithm 3, which produces a 512-bit message digest.

To specify a third combination, use the Add button beside the fields for the second combination.

VPN Zone

Select to create VPN zones. When enabled, you can select to create default or custom zones. When disabled, no VPN zones are created.

Create Default Zones

Select to have default zones created for you.

Use Custom Zone

Select to choose what zones to create.

IKE Security Phase 1 Advanced Properties

Diffie Hellman Group(s)

Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21.

At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.

Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

Exchange Mode

Select either *Aggressive* or *Main (ID Protection)*.

The FortiGate unit and the remote peer or dialup client exchange phase 1 parameters in either *Main (ID Protection)* or *Aggressive* mode. This choice does not apply if you use IKE version 2, which is available only for route-based configurations.

- In Main mode, the Phase 1 parameters are exchanged in multiple rounds with encrypted authentication information
- In Aggressive mode, the Phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

Although Main mode is more secure, you must select Aggressive mode if there is more than one dialup Phase 1 configuration for the interface IP address, and the remote VPN peer or client is authenticated using an identifier local ID). Descriptions of the peer options in this guide indicate whether Main or Aggressive mode is required.

Key Life

Type the time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172800 seconds.

Dead Peer Detection

Select this checkbox to reestablish VPN tunnels on idle connections and clean up dead IKE peers if required. You can use this option to receive notification whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.

IPsec Security Phase 2 Advanced Properties**Diffie Hellman Group(s)**

Select one or more of the following Diffie-Hellman (DH) groups: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21.

At least one of the DH group settings on the remote peer or client must match one the selections on the FortiGate unit. Failure to match one or more DH groups will result in failed negotiations.

Only one DH group is allowed for static and dynamic DNS gateways in aggressive mode.

Replay detection

Select to enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.

Perfect forward secrecy (PFS)	Select to enable or disable perfect forward secrecy (PFS). Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.
Key Life	Select the PFS key life. Select <i>Second</i> , <i>Kbytes</i> , or <i>Both</i> from the dropdown list and type the value in the text field.
Autokey Keep Alive	Select to enable or disable autokey keep alive. The phase 2 SA has a fixed duration. If there is traffic on the VPN as the SA nears expiry, a new SA is negotiated and the VPN switches to the new SA without interruption. If there is no traffic, the SA expires and the VPN tunnel goes down. A new SA will not be generated until there is traffic. The Autokey Keep Alive option ensures that a new SA is negotiated even if there is no traffic so that the VPN tunnel stays up.
Auto-Negotiate	Select to enable or disable auto-negotiation.
NAT Traversal	Select the checkbox if a NAT device exists between the local FortiGate unit and the VPN peer or client. The local FortiGate unit and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably.
Keep-alive Frequency	If NAT traversal is enabled or forced, type a keep-alive frequency setting (10-900 seconds).
Advanced-Options	For more information on advanced options, see the <i>FortiOS CLI Reference</i> .
DPD	Select to enable or disable DPD. You can also choose to set to <i>on-demand</i> or <i>on-idle</i> .
fcc-enforcement	Enable or disable FCC enforcement.
ike-version	Select the version of IKE to use. This is available only if IPsec Interface Mode is enabled. For more information about IKE v2, refer to RFC 4306. IKE v2 is not available if <i>Exchange Mode</i> is <i>Aggressive</i> . When IKE Version is set to 2, Mode and XAUTH are not available.
inter-vdom	Enable or disable the inter-vdom setting.
loccalid-type	Select the local ID type from the dropdown list. Select one of: <ul style="list-style-type: none"> <i>address</i>: IP Address <i>asn1dn</i>: ASN.1 Distinguished Name <i>auto</i>: Select type automatically <i>fqdn</i>: Fully Qualified Domain name <i>keyid</i>: Key Identifier ID <i>user-fqdn</i>: User Fully Qualified Domain Name
negotiate-timeout	Enter the negotiation timeout value. The default is 30 seconds.
npu-offload	Enable (default) or disable offloading of VPN session to a network processing unit (NPU).

View IPsec VPN community details

The VPN community information pane includes a quick status bar showing the community settings and the list of gateways in the community. Gateways can also be managed from this pane. See [IPsec VPN gateways on page 293](#) for information.

To view IPsec VPN community details:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the content pane. The community information pane opens.

Seq.#	Name	Role	Default VPN Interface	Protected Subnet
1	FGT54_2[root]	Spoke	wan2	10.2.1.0
2	FGT54_2[root]	Spoke	wan1	10.2.1.0
3	FGT54_1[root]	Hub	wan1	10.1.1.0
4	FGT54_1[root]	Hub	wan2	10.1.2.0

3. Select *All VPN Communities* in the tree menu to return to the VPN community list.

Editing an IPsec VPN community

To edit a VPN community, you must be logged in as an administrator with sufficient privileges. The community name and topology cannot be edited.

To edit IPsec VPN communities:

1. Go to *VPN Manager > IPsec VPN*.
2. Do one of the following:
 - Double-click on a community or select it in the tree menu, then click *Edit* in the quick status bar or select *VPN Community > Edit*.
 - Right-click on a community and select *Edit* from the menu.
 - Select a community, then click *Edit* in the toolbar.
 - The *Edit VPN Community* page is displayed.
3. Edit the settings as required, and then select *OK* to apply the changes.



For descriptions of the settings, see [VPN community settings on page 284](#).

Deleting VPN communities

To delete a VPN community or communities, you must be logged in as an administrator with sufficient privileges.

To delete VPN communities:

1. Go to *VPN Manager > IPsec VPN*.
2. Do one of the following:
 - Select the community in the tree, then select *VPN Community > Delete*.
 - Select the community or communities from the content pane list, then click *Delete* in the toolbar.
 - Select the community or communities from the content pane list, then right-click and select *Delete*.
3. Select *OK* in the confirmation box to delete the VPN community or communities.

Monitoring IPsec VPN tunnels

Go to *VPN Manager > Monitor* to view the list of IPsec VPN tunnels. You can also bring the tunnels up or down on this pane. Select a specific community from the tree menu to show only that community's tunnels.

<div><div><div><div><div></div></div><div>Refresh</div></div><div><div><div></div></div><div>Bring Tunnel Up</div></div><div><div><div></div></div><div>Bring Tunnel Down</div></div><div><div><div></div></div><div>Column Settings</div></div></div><div></div></div>								
<input type="checkbox"/>	Status	Device	Name	Type	Remote Gateway	Incoming Data	Phase 2 Proposal	Uptime
<input type="checkbox"/>	<div><div></div><div>Up</div></div>	FGT54_1[root]	dual-I_1_3	automatic	100.64.54.2	0.0 KB	1	1d 20h 39m 55s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_1_4	automatic	100.64.154.2	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_2_3	automatic	100.64.54.2	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_1[root]	dual-I_2_4	automatic	100.64.154.2	0.0 KB	1	15s
<input type="checkbox"/>	<div><div></div><div>Up</div></div>	FGT54_2[root]	dual-I_3_1	automatic	100.64.54.1	0.0 KB	1	1d 20h 39m 51s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_3_2	automatic	100.64.154.1	0.0 KB	1	2s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_4_1	automatic	100.64.54.1	0.0 KB	1	3s
<input type="checkbox"/>	<div><div></div><div>Down</div></div>	FGT54_2[root]	dual-I_4_2	automatic	100.64.154.1	0.0 KB	1	11s

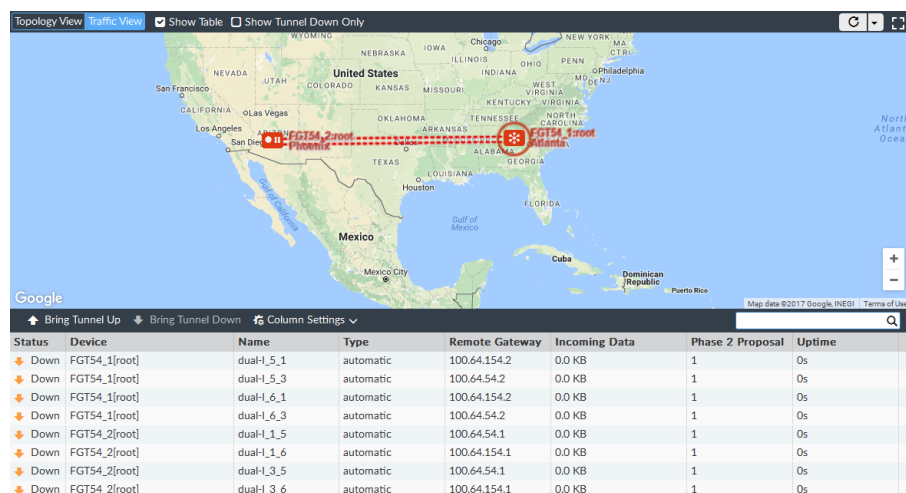
To bring tunnels up or down:

1. Go to *VPN Manager > Monitor*.
2. Find and select the tunnel or tunnels that you need to bring up or down in the list.
3. Click *Bring Tunnel Up* or *Bring Tunnel Down* from the toolbar or right-click menu
4. Select *OK* in the confirmation dialog box to apply the change.

Map View

The *Map View* pane shows IPsec VPN connections on an interactive world map (Google Maps). Select a specific community from the tree menu to show only that community's tunnels.

Hovering the cursor over a connection will highlight the connection and show the gateway, ADOM, and city names for each end of the tunnel.



The following options are available:

Topology View	The topology view shows the configured VPN gateways. See IPsec VPN gateways on page 293 .
Traffic View	The traffic view shows network traffic through the tunnels between protected subnets.
Show Table	<p>Select to show the connection table on the bottom of the pane. In the topology view, this option is only available when a specific community is selected.</p> <ul style="list-style-type: none"> The topology table shows the VPN gateway list and toolbar, with a column added for location. See Managing VPN gateways on page 293 for information. The traffic table shows the same information and options as the <i>Monitor</i> tab. See Monitoring IPsec VPN tunnels on page 291 for information.
Show Tunnel Down Only	<p>Select to show only tunnels that are currently down.</p> <p>This option is only available on the traffic view.</p>
Refresh	Click to refresh the map view, or click the down arrow and select a refresh rate from the dropdown menu.
Toggle Full Screen	Click to view the map in full screen mode. Press <i>Esc</i> to return to the windowed view.



If necessary, the location of a device can be manually configured when editing the device; see [Editing device information on page 139](#).

IPsec VPN gateways

A VPN gateway functions as one end of a VPN tunnel. It receives incoming IPsec packets, decrypts the encapsulated data packets, then passes the data packets to the local network. It also encrypts, encapsulates, and sends the IPsec data packets to the gateway at the other end of the VPN tunnel.

The IP address of a VPN gateway is usually the IP address of the network interface that connects to the Internet. You can also define a secondary IP address for the interface, and use that address as the local VPN gateway address, so that your existing setup is not affected by the VPN settings.

Once you have created the IPsec VPN topology, you can create managed and external gateways.

Managing VPN gateways

Go to *VPN Manager > IPsec VPN*, then select a community from the tree menu, or double-click on a community in the list, to manage the VPN gateways in that community.

Seq.#	Name	Role	Default VPN Interface	Protected Subnet
1	FGT54_2[root]	Spoke	wan2	10.2.1.0
2	FGT54_2[root]	Spoke	wan1	10.2.1.0
3	FGT54_1[root]	Hub	wan1	10.1.1.0
4	FGT54_1[root]	Hub	wan2	10.1.2.0

The following options are available:

Create New	Create a new managed or external gateway. See Creating managed gateways on page 293 and Creating external gateways on page 298 for more information.
Edit	Edit the selected gateway. See Editing an IPsec VPN gateway on page 299 .
Delete	Delete the selected gateway or gateways. See Deleting VPN gateways on page 299 .
Column Settings	Configure which columns are displayed, or click <i>Reset to Default</i> to reset the display to the default columns.
Search	Enter a search term to search the gateway list.

Creating managed gateways

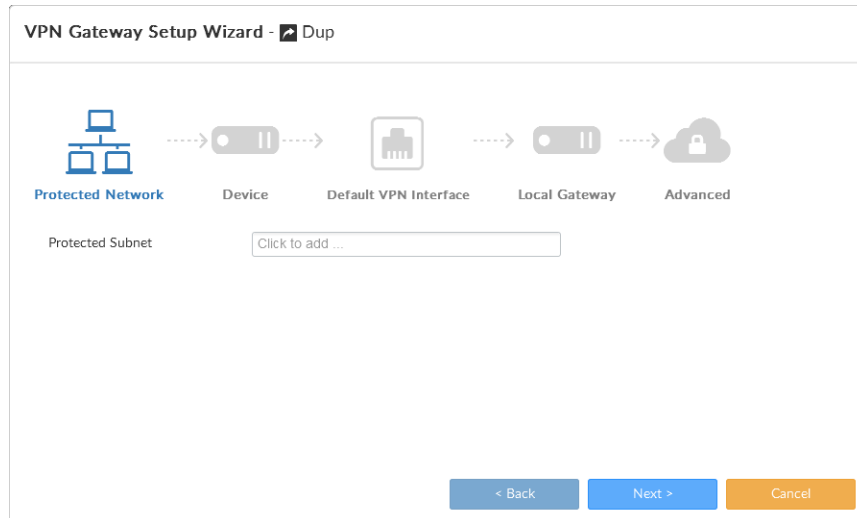
The settings available when creating a managed gateway depend on the VPN topology type, and how the gateway is configured.

Managed gateways are managed by FortiManager in the current ADOM. Devices in a different ADOM can be treated as external gateways. VPN configuration must be handled manually by the administrator in that ADOM. See [Creating external gateways on page 298](#).

To create a managed gateway:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the list.
3. On the community information content pane, in the toolbar, select *Create New > Managed Gateway*.

The *VPN Gateway Setup Wizard* opens.



4. Proceed through the five pages of the wizard, filling in the following values as required, then click **OK** to create the managed gateway.

Protected Subnet	Select a protected subnet from the dropdown list.
Role	Select the role of this gateway: <i>Hub</i> or <i>Spoke</i> . This option is only available for star and dial up VPN topologies.
Device	Select a device from the dropdown list.
Default VPN Interface	Select the interface to use for this gateway from the dropdown list.
Hub-to-Hub Interface	Select the interface to use for hub to hub communication. This is required if there are multiple hubs. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .
Local Gateway	Enter the local gateway IP address.
Local ID	Enter a local ID.
Routing	Select the routing method: <i>Manual (via Device Manager, or Automatic</i> .
Summary Network(s)	Select the network from the dropdown list and select the priority. Click the add icon to add more entries. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .

Peer Type	<p>Select one of the following:</p> <ul style="list-style-type: none"> • <i>Accept any peer ID</i> • <i>Accept this peer ID</i>: Enter the peer ID in the text field • <i>Accept a dialup group</i>: Select a group from the dropdown list <p>A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect.</p> <p>When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.</p> <p>The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID.</p> <p>This option is only available for dial up topologies.</p>
XAUTH Type	<p>Select the XAUTH type: <i>Disable</i>, <i>PAP Server</i>, <i>CHAP Server</i>, or <i>AUTO Server</i>.</p> <p>This option is only available for dial up topologies.</p>
User Group	<p>Select the authentication user group from the dropdown list.</p> <p>This field is available when <i>XAUTH Type</i> is set to <i>PAP Server</i>, <i>CHAP Server</i>, or <i>AUTO Server</i>.</p> <p>When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross referenced.</p>
Enable IKE Configuration Method ("mode config")	<p>Select to enable or disable IKE configuration method.</p> <p>This option is only available for dial up topologies.</p>
Enable IP Assignment	<p>Select to enable or disable IP assignment.</p> <p>This option is only available for dial up topologies. When the role is set to <i>Hub</i>, this option is only available when <i>Enable IKE Configuration Method</i> is on.</p>
IP Assignment Mode	<p>Select the IP assignment mode: <i>Range</i> or <i>User Group</i>.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.</p>
IP Assignment Type	<p>Select the IP assignment type: <i>IP</i> or <i>Subnet</i>.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.</p>
IPv4 Start IP	<p>Enter the IPv4 start IP address.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.</p>

IPv4 End IP	<p>Enter the IPv4 end IP address.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.</p>
IPv4 Netmask	<p>Enter the IPv4 netmask.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IP Assignment</i> turned on.</p>
Add Route	<p>Select to enable or disable adding a route for this gateway.</p> <p>This option is only available for dial up topologies.</p>
DNS Server #1 to #3	<p>Enter the DNS server IP addresses to provide IKE Configuration Method to clients.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and either <i>Enable IKE Configuration Method</i> turned on, or <i>DNS Service</i> is set to <i>Specify</i>.</p>
WINS Server #1 and #2	<p>Enter the WINS server IP addresses to provide IKE Configuration Method to clients.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.</p>
IPv4 Split include	<p>Select the address or address group from the dropdown list.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned on.</p>
Exclusive IP Range	<p>Enter the start and end IP addresses of the exclusive IP address range. Click the add icon to add more entries.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and either <i>Enable IKE Configuration Method</i> and <i>Enable IP Assignment</i> turned on, or <i>Enable IKE Configuration Method</i> turned off.</p>
DHCP Server	<p>Select to enable or disable DHCP server.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> is off.</p>
Default Gateway	<p>Enter the default gateway IP address.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.</p>
DNS Service	<p>Select <i>Use System DNS setting</i> to use the system's DNS settings, or <i>Specify</i> to specify DNS servers #1 to #3.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.</p>
Netmask	<p>Enter the netmask.</p> <p>This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.</p>

IPsec Lease Hold	Enter the IPsec lease hold time. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
Auto-Configuration	Select to enable or disable automatic configuration. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
DHCP Server IP Range	Enter the start and end IP addresses of the DHCP server range. Click the add icon to add more entries. This option is only available for dial up topologies with the role set to <i>Hub</i> and <i>Enable IKE Configuration Method</i> turned off.
Advanced	
authpasswd	Enter the XAuth client password for the FortiGate.
authusr	Enter the XAuth client user name for the FortiGate.
banner	Enter the banner value. Specify the message to send to IKE Configuration Method clients. Some clients display this message to users.
dns-mode	Select the DNS mode from the dropdown list: <ul style="list-style-type: none"> <i>auto</i>: Assign DNS servers in the following order: <ol style="list-style-type: none"> Servers assigned to interfaces by DHCP Per-VDOM assigned DNS servers Global DNS servers <i>manual</i>: Use the DNS servers specified in <i>DNS Server #1 to #3</i>.
domain	Enter the domain value.
public-ip	Enter the public IP address. Use this field to configure a VPN with dynamic interfaces. The value is the dynamically assigned PPPoE address that remains static and does not change over time.
route-overlap	Select the route overlap method from the dropdown list: <i>allow</i> , <i>use-new</i> , or <i>use-old</i> .
spoke-zone	Select a spoke zone from the dropdown list.
unity-support	Enable or disable unity support.
vpn-interface-priority	Set the VPN gateway interface priority. The default value is 1.
vpn-zone	Select a VPN zone from the dropdown list.

Creating external gateways

External gateways are not managed by the FortiManager device.

To create an external gateway:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the list.
3. On the community information content pane, in the toolbar, select *Create New > External Gateway*. The *New VPN External Gateway* pane opens.

4. Configure the following settings, then click *OK* to create the external gateway:

Node Type	Select either <i>HUB</i> or <i>Spoke</i> from the dropdown list. This option is only available for star and dial up VPN topologies.
Gateway Name	Enter the gateway name.
Gateway IP	Select the gateway IP address from the dropdown list.
Hub IP	Select the hub IP address from the dropdown list. This option is only available for star and dial up topologies with the role set to <i>Hub</i> .
Create Phase2 per Protected Subnet Pair	Toggle the switch to <i>On</i> to create a phase2 per protected subnet pair.
Routing	Select the routing method: <i>Manual (via Device Manager)</i> , or <i>Automatic</i> . This option is only available for full meshed and star topologies.

Peer Type

Select one of the following:

- *Accept any peer ID*
- *Accept this peer ID*: Enter the peer ID in the text field
- *Accept a dialup group*: Select a group from the dropdown list

A Local ID is an alphanumeric value assigned in the Phase 1 configuration. The local ID of a peer is called a Peer ID. The Local ID or peer ID can be used to uniquely identify one end of a VPN tunnel, enabling a more secure connection. If you have multiple VPN tunnels negotiating, this ensures the proper remote and local ends connect.

When you configure the ID on your end, it is your local ID. When the remote end connects to you, they see it as your peer ID. If you are debugging a VPN connection, the local ID is part of the VPN negotiations. You can use it to help troubleshoot connection problems.

The default configuration is to accept all local IDs (peer IDs). If your local ID is set, the remote end of the tunnel must be configured to accept your ID.

This option is only available for dial up topologies.

Protected Subnet

Select a protected subnet from dropdown list. You can add multiple subnets.

Local Gateway

Enter the local gateway IP address.

Editing an IPsec VPN gateway

To edit a VPN gateway, you must be logged in as an administrator with sufficient privileges. The gateway role and device (if applicable) cannot be edited.

To edit IPsec VPN communities:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the list.
3. Double-click on a gateway, right-click on a gateway and then select *Edit* from the menu, or select the gateway then click *Edit* in the toolbar. The *Edit VPN Gateway* pane opens.
4. Edit the settings as required, and then select *OK* to apply the changes.

Deleting VPN gateways

To delete a VPN gateway or gateways, you must be logged in as an administrator with sufficient privileges.

To delete VPN gateways:

1. Go to *VPN Manager > IPsec VPN*.
2. Select a community from the tree menu, or double-click on a community in the list.
3. Select the gateway or gateways you need to delete.
4. Click *Delete* in the toolbar, or right-click and select *Delete*.
5. Select *OK* in the confirmation box to delete the gateway or gateways.

VPN security policies

Once you have defined the IP source and destination addresses, the phase 1 authentication parameters, and the phase 2 parameters, you must define the VPN security policies.

FortiGate unit VPNs can be policy-based or route-based. There is little difference between the two types. In both cases, you specify phase 1 and phase 2 settings. However there is a difference in implementation. A route-based VPN creates a virtual IPsec network interface that applies encryption or decryption as needed to any traffic that it carries. That is why route-based VPNs are also known as interface-based VPNs. A policy-based VPN is implemented through a special security policy that applies the encryption you specified in the phase 1 and phase 2 settings.

An IPsec security policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, only a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel.

For a route-based VPN, you create two security policies between the virtual IPsec interface and the interface that connects to the private network. In one policy, the virtual interface is the source. In the other policy, the virtual interface is the destination. The *Action* for both policies is *Accept*. This creates bidirectional policies that ensure traffic will flow in both directions over the VPN.

For a policy-based VPN, one security policy enables communication in both directions. You must select *IPSEC* as the *Action* and then select the VPN tunnel dynamic object you have mapped to the phase 1 settings. You can then enable inbound and outbound traffic as needed within that policy, or create multiple policies of this type to handle different types of traffic differently. For example HTTPS traffic may not require the same level of scanning as FTP traffic.

Defining policy addresses

A VPN tunnel has two end points. These end points may be VPN peers, such as two FortiGate gateways. Encrypted packets are transmitted between the end points. At each end of the VPN tunnel, a VPN peer intercepts encrypted packets, decrypts the packets, and forwards the decrypted IP packets to the intended destination.

You need to define firewall addresses for the private networks behind each peer. You will use these addresses as the source or destination address depending on the security policy.

In general:

- In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant-tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer.
- In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer.

Defining security policies

Security policies allow IP traffic to pass between interfaces on a FortiGate unit. You can limit communication to particular traffic by specifying source and destination addresses. Then only traffic from those addresses will be allowed.

Policy-based and route-based VPNs require different security policies.

A policy-based VPN requires an IPsec security policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.

A route-based VPN requires an *Accept* security policy for each direction. As source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.

If the security policy that grants the VPN connection is limited to certain services, DHCP must be included, otherwise the client will not be able to retrieve a lease from the FortiGate's (IPsec) DHCP server because the DHCP request (coming out of the tunnel) will be blocked.

Before you define the IPsec policy, you must:

- Define the IP source and destination addresses.
- Specify the phase 1 authentication parameters.
- Specify the phase 2 parameters.
- Create a VPN Tunnel dynamic object (policy-based VPNs only).

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate unit, the FortiGate unit must be configured with an IPsec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate unit must evaluate IPSEC policies before ACCEPT and DENY security policies. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list. When you define multiple IPsec policies for the same tunnel, you must reorder the IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints.

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary Accept security policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs, which require IPsec security policies.

For more information on IPsec VPN, see the *FortiOS Handbook* in the [Fortinet Document Library](#). See [Managing policies on page 228](#) for information on creating policies on your FortiManager.

SSL VPN

You can use the *VPN Manager > SSL-VPN* pane to create and monitor Secure Sockets Layer (SSL) VPNs. You can also create and manage SSL VPN portal profiles.

Manage SSL VPNs

Go to *VPN Manager > SSL VPN* to manage SSL VPNs.

+ Create New Edit Delete			
Device	Interface	Port	Certificate
<input type="checkbox"/> FGT54_1	loop1,port1	10443	Fortinet_SSL
<input type="checkbox"/> FGT54_2	loop1,port1	10443	Fortinet_SSL

The following options are available:

Add SSL VPN

Create a new SSL VPN with the *Create SSL VPN* dialog box. See [Creating SSL VPNs on page 302](#).

Install Wizard	Launch the <i>Install Wizard</i> to install SSL VPN settings to devices.
Create New	Create a new SSL VPN with the <i>Create SSL VPN</i> pane. This option is also available from the right-click menu. See Creating SSL VPNs on page 302 .
Edit	Edit the selected VPN. This option is also available from the right-click menu. See Editing SSL VPNs on page 303 .
Delete	Delete the selected VPN or VPNs. This option is also available from the right-click menu. See Deleting SSL VPNs on page 304 .
Search	Enter a search term to search the VPN list.

Creating SSL VPNs

To create SSL VPNs, you must be logged in as an administrator with sufficient privileges. Multiple VPNs can be created.

To add SSL-VPN:

1. Go to *VPN Manager > SSL-VPN*.
2. Click *Add SSL VPN*, or click *Create New* in the content toolbar. The *Create SSL VPN* dialog box or pane is displayed.

3. Configure the following settings, then click *OK* to create the VPN.

Device	Select a FortiGate device or VDOM.
Connection Settings	Specify the connection settings.
Listen on Interface(s)	Define the interface the FortiGate will use to listen for SSL VPN tunnel requests. This is generally your external interface.
Listen on Port	Enter the port number for HTTPS access.

Restrict Access	Allow access from any hosts, or limit access to specific hosts. If limiting access, select the hosts that have access in the <i>Hosts</i> field.
Idle Logout	Select to enable idle timeout. When enabled, enter the amount of time that the connection can remain inactive before timing out, from 10 to 28800 seconds (default: 300) in the <i>Inactive For</i> field. This setting applies to the SSL VPN session. The interface does not time out when web application sessions or tunnels are up.
Server Certificate	Select the signed server certificate to use for authentication. Alternately, select a certificate template that is configured to use the FortiManager CA. See Certificate templates on page 158 .
Require Client Certificate	Select to use group certificates for authenticating remote clients. When the remote client initiates a connection, the FortiGate unit prompts the client for its client-side certificate as part of the authentication process. For information on using PKI to provide client certificate authentication, see the Authentication Guide.
Tunnel Mode Client Settings	Specify tunnel mode client settings. These settings determine how tunnel mode clients are assigned IP addresses.
Address Range	Either automatically assign address, or specify custom IP ranges.
DNS Server	Select to use the same DNS as the client system, or to specify DNS servers. Enter up to two DNS servers to be provided for the use of clients.
Specify WINS Servers	Select to specify WINS servers. Enter up to two WINS servers to be provided for the use of clients.
Allow Endpoint Registration	Select to allow endpoint registration.
Authentication/Portal Mapping	Select the users and groups that can access the tunnel.
Create New	Create a new authentication/portal mapping entry. Select the <i>Users</i> , <i>Groups</i> , <i>Realm</i> , and <i>Portal</i> , then click <i>OK</i> .
Edit	Edit the selected mapping.
Delete	Delete the selected mapping or mappings.
Advanced Options	Configure advanced SSL VPN options. For information, see the <i>FortiOS CLI Reference</i> : http://help.fortinet.com/cli/fos50hlp/56/index.htm .

Editing SSL VPNs

To edit an SSL VPN, you must be logged in as an administrator with sufficient privileges. The device cannot be edited.

To edit an SSL VPN:

1. Go to *VPN Manager > SSL VPN*.
2. Double-click on a VPN, right-click on a VPN and then select *Edit* from the menu, or select the VPN then click *Edit* in the toolbar. The *Create SSL VPN* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting SSL VPNs

To delete an SSL VPN or VPNs, you must be logged in as an administrator with sufficient privileges.

To delete SSL VPNs:

1. Go to *VPN Manager > SSL VPN*.
2. Select the VPN or VPNs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the selected VPN or VPNs.

Portal profiles

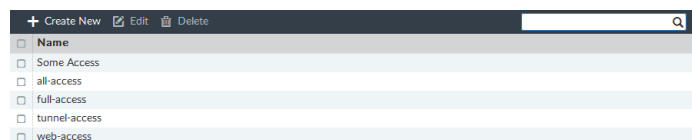
The SSL VPN portal enables remote users to access internal network resources through a secure channel using a web browser. FortiGate administrators can configure login privileges for system users as well as the network resources that are available to the users.

There are three pre-defined default portal profiles:

- Full-access
- Tunnel-access
- Web-access

Each portal type includes similar configuration options. You can also create custom portal profiles.

To manage portal profiles, go to *VPN Manager > SSL VPN* and select *Portal Profiles* in the tree menu.



The following options are available:

Create New	Create a new portal profile.
Edit	Edit the selected profile.
Delete	Delete the selected profile or profiles.
Search	Enter a search term to search the portal profile list.

Creating SSL VPN portal profiles

To create SSL VPN portal profiles, you must be logged in as an administrator with sufficient privileges. Multiple profiles can be created.

To create portal profiles:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Click *Create New* in the toolbar, or right-click and select *Create New*. The *Create New* pane is displayed.

Create New Portal Profile

Name

Limit Users to One SSL VPN Connection at a Time ☒

Tunnel Mode ☒

Enable Split Tunneling ☒

Routing Address

Source IP Pools

IPv6 Tunnel Mode ☒

IPv6 Split Tunneling ☒

IPv6 Routing Address

Source IPv6 Pools

Tunnel Mode Client Options

Allow client to save password ☒

Allow client to connect automatically ☒

Allow client to keep connections alive ☒

Enable Web Mode ☒

Portal Message

Theme

Show Session Information

Show Connection Launcher

Show Login History

User Bookmarks

Predefined Bookmarks

+ Create New ☒ Edit ☐ Delete ☐

Name	Type	Location	Description
Enable FortiClient Download	<input checked="" type="checkbox"/>		
Download Method	<input checked="" type="checkbox"/>	Direct	SSL-VPN Proxy
Customize Download Location	<input type="checkbox"/>		

Advanced Options >

OK Cancel

3. Configure the following settings, then select *OK* to create the profile.

Name	Enter a name for the portal.
Limit Users to One SSL VPN Connection at a Time	Set the SSL VPN tunnel so that each user can only be logged in to the tunnel one time per user log in. Once they are logged in to the portal, they cannot go to another system and log in with the same credentials until they log out of the first connection.
Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv4 addresses.
Enable Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.

Routing Address	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.
Source IP Pools	Select an IPv4 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
IPv6 Tunnel Mode	Select to configure and enable tunnel mode access. These settings determine how tunnel mode clients are assigned IPv6 addresses.
Enable IPv6 Split Tunneling	Select so that the VPN carries only the traffic for the networks behind the FortiGate unit. The user's other traffic follows its normal route.
IPv6 Routing Address	If you enable split tunneling, you are required to set the address that your corporate network is using. Traffic intended for the routing address will not be split from the tunnel.
Source IP Pools	Select an IPv6 pool for users to acquire an IP address when connecting to the portal. There is always a default pool available if you do not create your own.
Tunnel Mode Client Options	These options affect how the FortiClient application behaves when connected to the FortiGate VPN tunnel. When enabled, a checkbox for the corresponding option appears on the VPN log in screen in FortiClient, and is disabled by default.
Allow client to save password	The user's password is stored on the user's computer and will automatically populate each time they connect to the VPN.
Allow client to connect automatically	When the FortiClient application is launched, for example after a reboot or system start up, FortiClient will automatically attempt to connect to the VPN tunnel.
Allow client to keep connections alive	The FortiClient connection will not shut down. When not selected, during periods of inactivity, FortiClient will attempt to stay connected every three minutes for a maximum of 10 minutes.
Enable Web Mode	Select to enable web mode access.
Portal Message	The text header that appears on the top of the web portal.
Theme	A color styling specifically for the web portal: <i>blue</i> , <i>green</i> , <i>mariner</i> , <i>melongene</i> , or <i>red</i> .
Show Session Information	Display the <i>Session Information</i> widget on the portal page. The widget displays the log in name of the user, the amount of time the user has been logged in, and the inbound and outbound traffic statistics.
Show Connection Launcher	Display the <i>Connection Launcher</i> widget on the portal page. Use the widget to connect to an internal network resource without adding a bookmark to the bookmark list. You select the type of resource and specify the URL or IP address of the host computer.
Show Login History	Include user log in history on the web portal, then specify the number of history entries.

User Bookmarks	Include bookmarks on the web portal. Bookmarks are used as links to internal network resources. When a bookmark is selected from a bookmark list, a pop-up window opens with the web page. Telnet, VNC, and RDP require a browser plugin. FTP and Samba replace the bookmarks page with an HTML file-browser.
Pre-Defined Bookmarks	The list of predefined bookmarks. Click <i>Create New</i> to add a bookmark. See Predefined bookmarks on page 307 for information.
Enable FortiClient Download	Select to enable FortiClient downloads.
Download Method	Select the method to use for downloading FortiClient from the SSL VPN portal. Choose between <i>Direct</i> and <i>SSL-VPN Proxy</i> . This option is only available when FortiClient download is enabled.
Customize Download Location	Select to specify a custom location to use for downloading FortiClient. You can specify a location for FortiClient (Windows) and FortiClient (Mac OS X). Type the URL in the <i>Windows</i> box and/or <i>Mac</i> box. This option is only available when FortiClient download is enabled.
Advanced Options	Configure advanced options. For information, see the <i>FortiOS CLI Reference</i> : http://help.fortinet.com/cli/fos50hlp/56/index.htm .

Predefined bookmarks

Bookmarks are used as links to specific resources on the network. When a bookmark is selected from a bookmark list, a window opens with the requested web page. Telnet, RDP, and VNC open a window that requires a browser plug-in. FTP replaces the bookmark page with an HTML file-browser.

A web bookmark can include log in credentials to automatically log the SSL VPN user into the web site. When the administrator configures bookmarks, the web site credentials must be the same as the user's SSL VPN credentials. Users configuring their own bookmarks can specify alternative credentials for the web site.

Predefined bookmarks can be added to portal profiles when creating or editing a profile.

To create a predefined bookmark:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 309](#) or [Creating SSL VPN portal profiles on page 305](#).
3. Click *Create New* in the *Pre-Defined Bookmark* field. *Enable Web Mode* must be selected for this field to be available. The *Create New Bookmark* dialog box opens. The available options will vary depending on the selected type.

Create New Bookmark

Name

Type

Port Forward

Host

Remote Port

Listening Port

Show Status Window

ON

Description

OK

Cancel

4. Configure the following settings, then select **OK** to create the bookmark.

Name	Enter a name for the bookmark.
Type	Select the bookmark type: <i>CITRIX</i> , <i>FTP</i> , <i>Port Forward</i> , <i>RDP</i> , <i>SMB</i> , <i>SSH</i> , <i>Telnet</i> , or <i>VNC</i> , <i>HTTP/HTTPS</i> .
URL	Enter the bookmark URL. This option is only available when <i>Type</i> is <i>Citrix</i> , or <i>HTTP/HTTPS</i> .
Folder	Enter the bookmark folder. This option is only available when <i>Type</i> is <i>FTP</i> , or <i>SMB</i> .
Host	Enter the host name. This option is only available when <i>Type</i> is <i>RDP</i> , <i>SSH</i> , <i>TELNET</i> , or <i>VNC</i> .
Remote Port	Enter the remote port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Listening Port	Enter the listening port. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Show Status Window	Enable to show the status window. This option is only available when <i>Type</i> is <i>Port Forward</i> .
Port	Enter the port number. This option is only available when <i>Type</i> is <i>RDP</i> , or <i>VNC</i> .
Username	Enter the user name. This option is only available when <i>Type</i> is <i>RDP</i> .
Password	Enter the password. This option is only available when <i>Type</i> is <i>RDP</i> , or <i>VNC</i> .
Keyboard Layout	Select the keyboard layout: <i>German (QWERTZ)</i> , <i>English (US)</i> , <i>Unknown</i> , <i>French (AZERTY)</i> , <i>Italian</i> , or <i>Swedish</i> . This option is only available when <i>Type</i> is <i>RDP</i> .

Security	<p>Select the security type: <i>Allow the server to choose the type of security</i>, <i>Network Level Authentication</i>, <i>Standard RDP encryption</i>, or <i>TLS encryption</i>.</p> <p>This option is only available when <i>Type</i> is <i>RDP</i>.</p>
Description	<p>Optionally, enter a description of the bookmark.</p>
Single Sign-on	<p>Select the SSO setting for links that require authentication: <i>Disabled</i>, <i>Automatic</i>, or <i>Static</i>. <i>Static</i> is only available when <i>Type</i> is <i>Citrix</i> or <i>HTTP/HTTPS</i>.</p> <p>If <i>Static</i> is selected, click the add icon, then enter the <i>Name</i> and <i>Value</i> to add SSO Form Data. Multiple fields can be added. Click <i>Remove</i> to remove a field.</p> <p>When including a link using SSO, use the entire URL and not just the IP address.</p> <p>This option is only available when <i>Type</i> is <i>Citrix</i>, <i>FTP</i>, <i>SMB</i>, or <i>HTTP/HTTPS</i>.</p>

To edit a bookmark:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 309](#) or [Creating SSL VPN portal profiles on page 305](#).
3. Click the *Edit* icon in the bookmark row. The *Bookmark* dialog box opens.
4. Edit the bookmark as required, then click *OK* to apply your changes.

To delete a bookmark:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Edit an existing profile, or create a new profile. See [Editing portal profiles on page 309](#) or [Creating SSL VPN portal profiles on page 305](#).
3. Click the *Delete* icon in the bookmark row.

Editing portal profiles

To edit a portal profile, you must be logged in as an administrator with sufficient privileges. The device cannot be edited.

To edit a portal profile:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Double-click on a profile, right-click on a profile and then select *Edit* from the menu, or select the profile then click *Edit* in the toolbar. The *Edit Portal Profile* pane opens.
3. Edit the settings as required, and then select *OK* to apply the changes.

Deleting portal profiles

To delete a portal profile or profiles, you must be logged in as an administrator with sufficient privileges.

To delete portal profiles:

1. Go to *VPN Manager > SSL-VPN* and select *Portal Profiles* in the tree menu.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Select *OK* in the confirmation box to delete the selected profile or profiles.

Monitor SSL VPNs

SSL VPNs can be monitored by going to *VPN Manager > SSL VPN* and selecting *Monitor* from the tree menu.

The following information is shown:

Device	The device or VDOM name.
User	The user name.
Remote Host	The remote host.
Last Login	The time of the last log in.
Active Connections	The number of active connections on the VPN.

AP Manager

Use *AP Manager* to manage FortiAP access points.

The AP Manager pane includes the following tabs:

Managed APs	Displays unauthorized and authorized FortiAP devices. You can view, authorize unauthorized FortiAP devices, and edit authorized FortiAP devices.
Monitoring AP devices	Monitor FortiAP devices and the clients connected to them.
Map View	View the locations of FortiAP devices on a map.
WiFi templates	View, create, edit, and import AP profiles, SSIDs, and WIDS profiles.

The AP Manager pane allows you to manage, configure, and assign profiles to FortiAP devices. You can configure multiple profiles that can be assigned to multiple devices. Profiles are installed to devices when you install configurations to the devices.

In central management mode, WiFi templates share a common database. Templates can be applied to any device, regardless of which FortiGate controller it is connected to. In per-device mode, all FortiAP devices and WiFi templates (SSIDs, WIDS profiles, and AP profiles) are managed at the device level – there are no shared objects. The monitor and map view tabs will only show information for FortiAP devices connected to the selected FortiGate controller. The mode can be changed by editing the ADOM that contains the FortiGate controllers ([Creating ADOMs on page 57](#)).

The following steps provide an overview of using AP management to configure and install profiles:

1. Create AP profiles.
See [WiFi templates on page 324](#).
2. Assign profiles to FortiAP devices.
See [Assigning profiles to FortiAP devices on page 318](#).
3. Install FortiAP profiles to devices.
On the *Device Manager* pane, select the FortiGate device that controls the FortiAP device, then select *Install > Install Config* from the toolbar, and follow the prompts in the wizard. See [Configuring a device on page 125](#).

Managed APs

The *Managed APs* pane allows you to manage FortiAP devices that are controlled by FortiGate devices that are managed by the FortiManager.

FortiAP devices, listed in the tree menu, are grouped based on the controller that they are connected to. The devices can also be further divided into platform based groups within a controller.

FortiAP devices can be managed centrally, or per-device (see [Creating ADOMs on page 57](#)). In per-device mode, all WiFi profiles (SSIDs, WIDS profiles, and AP profiles), as well as managed FortiAP devices, are managed at the device level – there are no shared objects.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click on the mouse on different parts of the navigation panes on the GUI page to access these context menus.



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 64](#).

Go to *AP Manager > Managed APs* to manage FortiAP devices. Managed APs are organized by their FortiGate controller and group. In per-device mode, there is no *All_FortiGate* group.

Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
FAP2283U111111111	192.168.1.110		Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	FAP228-v5.2-build0000	
FP320B00000000000	192.168.1.112		Radio 1: 36 Radio 2: 11	Radio 1: 0 Radio 2: 1	FP320B-v5.2-build0000	
FWF92D-WIFI0	127.0.0.1		Radio 1: 6 Radio 2: 0	Radio 1: 0 Radio 2: 0	FWF92D-v5.4-build0000	
PS321C00000000000	192.168.100.113		Radio 1: 1 Radio 2: 165	Radio 1: 0 Radio 2: 0	PS321C-v5.4-build0000	

Quick status bar

You can quickly view the status of devices on the *Managed AP* pane by using the quick status bar, which contains the following options:

- Managed APs
- Online
- Offline
- Unauthorized
- Rogue APs
- Client Connected

You can click each quick status to display in the content pane, or in a pop-up window, only the devices referenced in the quick status.

To view the quick status bar:

1. Ensure that you are in the correct ADOM.
2. Go to *AP Manager > Managed APs*. The quick status bar is displayed above the content pane.

3. In the tree menu, select a FortiGate, group, or *All_FortiGate* if central management is enabled. The devices for the group are displayed in the content pane, and the quick status bar updates.
4. Click on each quick status to filter the devices displayed on the content pane. For example, click *Offline*, and the content pane will display only devices that are currently offline.

5. Click *Rogue APs* to open the rogue AP list in a pop-up window.
6. Click *Client Connected* to open a list of WiFi clients in a pop-up window.

Managing APs

FortiAP devices can be managed from the content pane below the quick status bar on the *AP Manager > Managed APs* pane.

+ Create New Edit Delete Assigned Profile Column Settings More						
<input type="checkbox"/>	Access Point	Connected Via	SSIDs	Channel	Clients	OS Version
<input type="checkbox"/>	FAP22B3U111111111	192.168.1.110	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0	FAP22B-v5.2-build0000
<input type="checkbox"/>	FP320B0000000000	192.168.1.112	Radio 1: Radio 2:	Radio 1: 36 Radio 2: 11	Radio 1: 0 Radio 2: 1	FP320B-v5.2-build0000
<input type="checkbox"/>	FWF92D-WIFI0	127.0.0.1	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 0	Radio 1: 0 Radio 2: 0	FWF92D-v5.4-build0000
<input type="checkbox"/>	PS321C0000000000	192.168.100.113	Radio 1: Radio 2:	Radio 1: 1 Radio 2: 165	Radio 1: 0 Radio 2: 0	PS321C-v5.4-build0000

The following options are available from the toolbar and right-click menu:

Create New	Add an AP.
Edit	Edit the selected AP.
Delete	Delete the selected AP.
Assigned Profile	Assign a profile from the list to the AP. Only applicable profiles will be listed. See Assigning profiles to FortiAP devices on page 318 .
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
Authorize	Authorize an unregistered AP. See Authorizing and deauthorizing FortiAP devices on page 318 . This option is also available in the toolbar by selecting <i>More</i> .
Deauthorize	Deauthorize a registered AP. See Authorizing and deauthorizing FortiAP devices on page 318 . This option is also available in the toolbar by selecting <i>More</i> .
Grouping	Move the selected FortiAP devices into a new group. The APs must be the same model to be grouped. See FortiAP groups on page 317 . This option is only available in the right-click menu.
Upgrade	Upgrade the AP. The AP must already be authorized.
Restart	Restart the AP. This option is only available in the toolbar, by selecting <i>More</i> .
Refresh	Refresh the AP list, or refresh the selected FortiAP devices.
View Clients	View the clients connected to the AP. See Connected clients on page 320 .

View Rogue APs	View the Rogue APs. See Rogue APs on page 318 . This option is only available in the toolbar, by selecting <i>More</i> .
Search	Enter a search string into the search field to search the AP list. This option is only available in the toolbar.

The following information is available in the content pane:

FortiGate	The FortiGate unit that is managing the AP.
Access Point	The serial number of the AP.
Connected Via	The IP address of the AP.
SSIDs	The SSIDs associated with the AP.
Channel	The wireless radio channels that the access point uses.
Clients	The number of clients connected to the AP. Select a value to open the View WiFi Clients window to view more details about the clients connected to that radio. See Connected clients on page 320 .
OS Version	The OS version on the FortiAP.
AP Profile	The AP Profile assigned to the device, if any.
Comments	User entered comments.
Country	The Country code that the FortiAP is using.
Join Time	The date and time that the FortiAP joined.
LLDP	The Link Layer Discovery Protocol
Operating TX Power	The transmit power of the wireless radios.
Serials #	The serial number of the device
WTP Mode	The Wireless Transaction Protocol (WTP) mode, or <i>0</i> if none.

To add a FortiAP:

1. Click *Create New* on the content pane toolbar. The *Add FortiAP* dialog box opens.

Add FortiAP

FortiGate

Click to select ▼

Serials Number

Name

AP Profile

OK

Cancel

2. Enter the following information:

FortiGate	Select the FortiGate that the AP will be added to from the dropdown list. If you have already selected a FortiGate in the tree menu, this field will contain that FortiGate.
Serials Number	Enter the device's serial number.
Name	Enter a name for the device.
AP Profile	Select an AP profile to apply to the device from the dropdown list. See AP profiles on page 324 .

3. Click *OK* to add the device.

To edit FortiAP devices:

1. In the tree menu, select the group or FortiGate that contains the FortiAP device to be edited.
2. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
3. Either select the FortiAP and click *Edit* from the toolbar, double-click on the FortiAP, or right-click on the FortiAP and select *Edit*. The *Config FortiAP* window opens.

Config FortiAP - FP320B3X00000000

Serial Number
FP320B3X00000000
Name
FP320B3X00000000
Comments
Write a comment
0/255

Managed AP Status
Status
Idle
Connected Via
Ethernet(0.0.0.0)
Base MAC Address
00:00:00:00:00:00
Join Time
Clients
0
FortiAP OS Version
Upgrade
State
Authorized

Wireless Settings
FortiAP Profile
FAP320B-default
Override Settings
Enable WiFi Radio
SSID
Automatically Inherit all SSIDs
Select SSIDs
Click to add...
Auto TX Power Control
Disable
Enable
TX Power
0%
Do not participate in Rogue AP scanning
LAN Port
Mode
None
Bridge to
Radio Settings Summary

Radio	Setting	Channels	SSIDs
Radio 1	AP	Automatically Selected	
Radio 2	AP(2.4GHz 802.11n/g/b)	Automatically Selected	

OK
Cancel

4. Edit the following options:

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the AP.
Comments	Comments about the AP, such as its location or function.
Managed AP Status	Various information about the AP.
Status	The status of the AP, such as <i>Connected</i> , or <i>Idle</i> .
Connected Via	The method by which the device is connected to the controller.
Base MAC Address	The MAC address of the device.
Join Time	The time that the AP joined.
Clients	The number of clients currently connected to the AP.
FortiAP OS Version	The AP's current firmware version. Select <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available. See Firmware Management on page 152
State	The state of the AP, such as <i>Authorized</i> , or <i>Discovered</i> .
Wireless Settings	Assign a profile or configure radio settings manually.
FortiAP Profile	Select a profile from the dropdown list (see AP profiles on page 324), or select <i>Override Settings</i> to customize the WiFi radio settings for the AP (SSIDs, TX Power, and Rogue AP Scanning).
Do not participate in Rogue AP scanning	Select this option to not participate in scanning for rogues APs.
Radio Settings Summary	A table showing the current setting, channels, and SSIDs configured for the AP's radio or radios.

5. Click *Apply* to apply your changes.**To delete FortiAP devices:**

1. In the tree menu, select the group or FortiGate that contains the FortiAP device to be deleted.
2. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
3. Either select the FortiAP and click *Delete* from the toolbar, or right-click on the FortiAP and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the AP.



A FortiAP device cannot be deleted if it is currently being used. For example, if a firewall profile has been assigned to it.

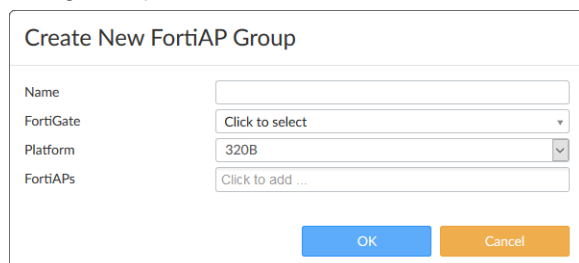
FortiAP groups

FortiAP devices can be organized into groups based on FortiAP platforms. A group can only contain one model of FortiAP. A FortiAP can only belong to one group.

Groups are listed in the tree menu under the FortiGate they were created in. They can be created, edited, and deleted as needed.

To create a FortiAP group:

1. In the *Managed APs* pane, select *FortiAP Group > Create New* from the toolbar. The *Create New FortiAP Group* dialog box opens.



The dialog box titled "Create New FortiAP Group" contains the following fields:

- Name:** A text input field.
- FortiGate:** A dropdown menu with the text "Click to select".
- Platform:** A dropdown menu with "320B" selected.
- FortiAPs:** A text input field with the text "Click to add ...".

At the bottom right are two buttons: "OK" (blue) and "Cancel" (orange).

2. Configure the following:

Name	Enter a name for the group.
FortiGate	Select the FortiGate under which the group will be created.
Platform	Select the FortiAP platform that the group will apply to.
FortiAPs	Select FortiAPs to add to the group. Only FortiAPs in the selected FortiGate of the selected platform will be available for selection.

3. Select *OK* to create the group.

To edit a group:

1. In the *Managed APs* pane, select a group from the tree menu, then select *FortiAP Group > Edit* from the toolbar.
2. Edit the group name and devices in the group as needed. The FortiGate and the platform cannot be changed.
3. Select *OK* to apply your changes.

To delete a group:

1. In the *Managed APs* pane, select a group from the tree menu.
2. Select *FortiAP Group > Delete* from the toolbar.
3. Select *OK* in the confirmation dialog box to delete the group.

Authorizing and deauthorizing FortiAP devices

To authorize FortiAP devices:

1. In the tree menu, select the group or FortiGate that contains the unauthorized FortiAP devices.
2. In the quick status bar, click *Unauthorized*. The unauthorized FortiAP devices are displayed in the content pane.
3. Select the FortiAP devices and either click *More > Authorize* from the toolbar, or right-click and select *Authorize*.
4. Select *OK* in the confirmation dialog box to authorize the selected devices.

To deauthorize FortiAP devices:

1. In the tree menu, select the group or FortiGate that contains the FortiAP devices to be deauthorized
2. Select the FortiAP devices and either click *More > Deauthorize* from the toolbar, or right-click and select *Deauthorize*.
3. Select *OK* in the confirmation dialog box to deauthorize the selected devices.

Assigning profiles to FortiAP devices

You use the AP Manager pane to assign profiles to FortiAP devices, and you use the Device Manager pane to install profiles to FortiAP devices when you install a configuration to the FortiGate that controls the FortiAP device.

For more information about creating and managing AP profiles, see [AP profiles on page 324](#).

To assign profiles to FortiAP devices:

1. In the tree menu, select the group or FortiGate that contains the FortiAP device the profile will be applied to.
2. Locate the FortiAP device in the list in the content pane, or refine the list by selecting an option from the quick status bar.
3. Either select the FortiAP and click *Assigned Profile* from the toolbar, or right-click on the FortiAP and select *Assigned Profile*. The *Assign AP Profile* window opens.
4. Select a FortiAP profile from the dropdown list, then click *OK* to assign the profile.

To install FortiAP profiles to devices:

1. Go to the *Device Manager* pane.
2. Select the FortiGate device that controls the FortiAP device
3. Right click and select *Install Config*, or select *Install > Install Config* from the toolbar.
4. Click *OK* in the confirmation dialog box to install the configuration to the device. See [Configuring a device on page 125](#) for more information.

Rogue APs

A rogue AP is an unauthorized AP connected to your wired network. This can enable unauthorized access.

Click *Rogue APs* in the quick status bar to open the rogue AP list in a pop-up window.

View Rogue APs

<input checked="" type="checkbox"/> Mark As <input checked="" type="checkbox"/> Suppress AP <input checked="" type="checkbox"/> Unsuppress AP <input checked="" type="checkbox"/> Refresh <input checked="" type="checkbox"/> Column Settings										
State	Status	SSID	Security Type	Channel	MAC Address	Vendor Info	Signal Strength	Detected By	On-Wire	
<input type="checkbox"/>		QA-Forticlient57	WPA2 Personal	6	00:02:6f:f8:f9:a7	Senao International	-74 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		fortinet	WPA2 Personal	161	00:02:6f:f8:f9:a7	Senao International	-50 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		FWF40C-vap09-mesh	WPA2 Personal	6	00:09:0f:44:b0:95	Fortinet Inc.	-83 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		RA-Lab	WPA2 Personal	6	00:09:0f:4c:d4:05	Fortinet Inc.	-81 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		test-test	WPA/WPA2 Personal	6	00:09:0f:8c:ec:da	Fortinet Inc.	-31 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		FG200P.mesh.vd1	WPA Personal	161	00:09:0f:8d:a9:e6	Fortinet Inc.	-45 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		FG200P.user.mesh	WPA2 Personal	3	00:09:0f:9e:c7:82	Fortinet Inc.	-36 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		fortinet.local.br	WPA2 Personal	11	00:09:0f:9f:95:07	Fortinet Inc.	-46 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		Farshad-SSID	WPA2 Personal	1	00:09:0f:a1:94:47	Fortinet Inc.	-76 dBm	FP320C3X15000146	(1)	
<input type="checkbox"/>		FTNT-Staff-test	WPA/WPA2 Enterprise	1	00:09:0f:a5:fa:a0	Fortinet Inc.	-76 dBm	FP320C3X15000146	(1)	

Close

The following options are available:

Mark As

Mark a rogue AP as:

- **Accepted:** for APs that are an authorized part of your network or are neighboring APs that are not a security threat.
- **Rogue:** for unauthorized APs that On-wire status indicates are attached to your wired networks.
- **Unclassified:** the initial status of a discovered AP. You can change an AP back to unclassified if you have mistakenly marked it as **Rogue** or **Accepted**.

Suppress AP

Suppress the selected APs. This will prevent users from connecting to the AP. When suppression is activated against an AP, the controller sends deauthentication messages to the rogue AP's clients posing as the rogue AP, and also sends deauthentication messages to the rogue AP posing as its clients. Before enabling this feature, verify that operation of Rogue Suppression is compliant with the applicable laws and regulations of your region.

Unsuppress AP

Turn of suppression for the selected rogue APs.

Refresh

Refresh the rogue AP list.

Column Settings

Click to select which columns to display or select *Reset to Default* to display the default columns.

The following columns are available:

State

The state of the AP:

- Suppressed: red suppressed icon
- Rogue: orange rogue icon
- Accepted: green wireless signal mark
- Unclassified: gray question mark

Status

Whether the AP is active (green) or inactive (orange).

SSID

The wireless service set identifier (SSID) or network name for the wireless interface.

Security Type

The type of security currently being used.

Channel	The wireless radio channel that the access point uses.
MAC Address	The MAC address of the wireless interface.
Vendor Info	The name of the vendor.
Signal Strength	The relative signal strength of the AP.
Detected By	The name or serial number of the AP unit that detected the signal.
On-Wire	A green up-arrow indicates a suspected rogue, based on the on-wire detection technique. An orange down-arrow indicates AP is not a suspected rogue.
First Seen	How long ago this AP was first detected. This column is not visible by default.
Last Seen	How long ago this AP was last detected. This column is not visible by default.
Rate	The data rate in, bps. This column is not visible by default.

Connected clients

To view connected wireless clients, click *Client Connected* in the quick status bar to open the WiFi client list in a pop-up window that lists all the clients in the selected FortiGate or group.

To view the clients connected to specific APs, select the APs in the content pane, then right-click on them and select *View Clients*.

SSID	FortiAP	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal Strength	Association Time
test-test11	FP32080000000000	192.168.168.1	[device icon]	00:00:00:00:00:00	11	0 kbps	16 dB	16/16/16 16:16

The following columns are available:

SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit that the client connected to.
IP	The IP address assigned to the wireless client.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.
Association Time	How long the client has been connected to this access point.

Authentication	The type of authentication used.
Bandwidth RX	Client received bandwidth, in Kbps.
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The OS version on the FortiAP.
Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.
Name	The name of the FortiGate device that the FortiAP is attached to.

Monitoring AP devices

The *Monitor* pane includes a listing of connected clients, and a health monitor that display information about all the APs for the selected FortiGate or group in widgets.

Clients Monitor

The client monitor lists information about connected clients. Go to *AP Manager > Monitor* and select the *Clients Monitor* tab in the content pane to view the list. Select a specific FortiGate or group in the tree menu to filter the listed clients.

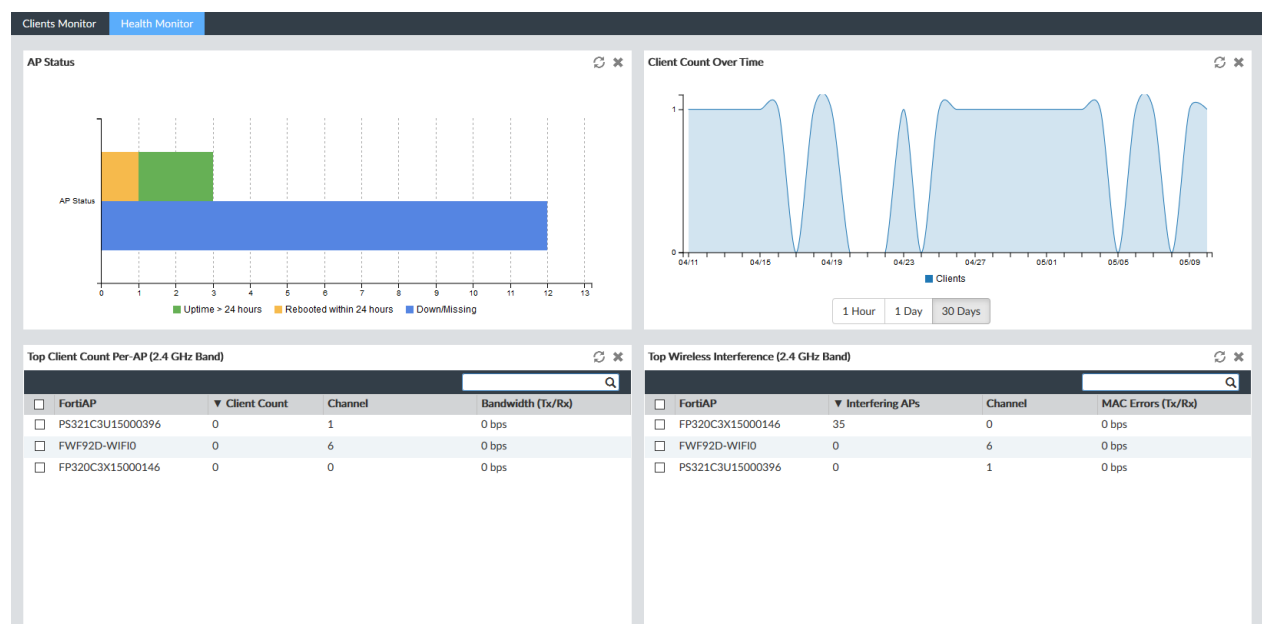
You can search the table by entering a search term in the search field in the toolbar. The visible columns can be adjusted by selecting *Column Settings* in the toolbar. The following columns are available:

SSID	The SSID that the client connected to.
FortiAP	The serial number of the FortiAP unit that the client connected to.
IP	The IP address assigned to the wireless client.
Device	The type of device that the client is using.
Channel	The wireless radio channel that is used.
Bandwidth Tx/Rx	Client received and transmitted bandwidth, in Kbps.
Signal Strength/Noise	The signal-to-noise ratio in dBs calculated from signal strength and noise level.
Signal Strength	The relative signal strength of the AP.
Association Time	How long the client has been connected to this access point.
Auth	The type of authentication used.

Bandwidth RX	Client received bandwidth, in Kbps.
Bandwidth TX	Client transmitted bandwidth, in Kbps.
Device OS	The OS version on the FortiAP.
Host Information	The host name of the WiFi client, if available.
Idle Time	The amount of time that the client has been idle.
Manufacturer	The manufacturer of the client device.
Rate	The connection rate between the WiFi client and the AP.
Name	The name of the FortiGate device that the FortiAP is attached to.

Health Monitor

Go to *AP Manager > Monitor*, select a FortiGate or group from the tree menu, and select the *Health Monitor* tab in the content pane to open the health monitor.



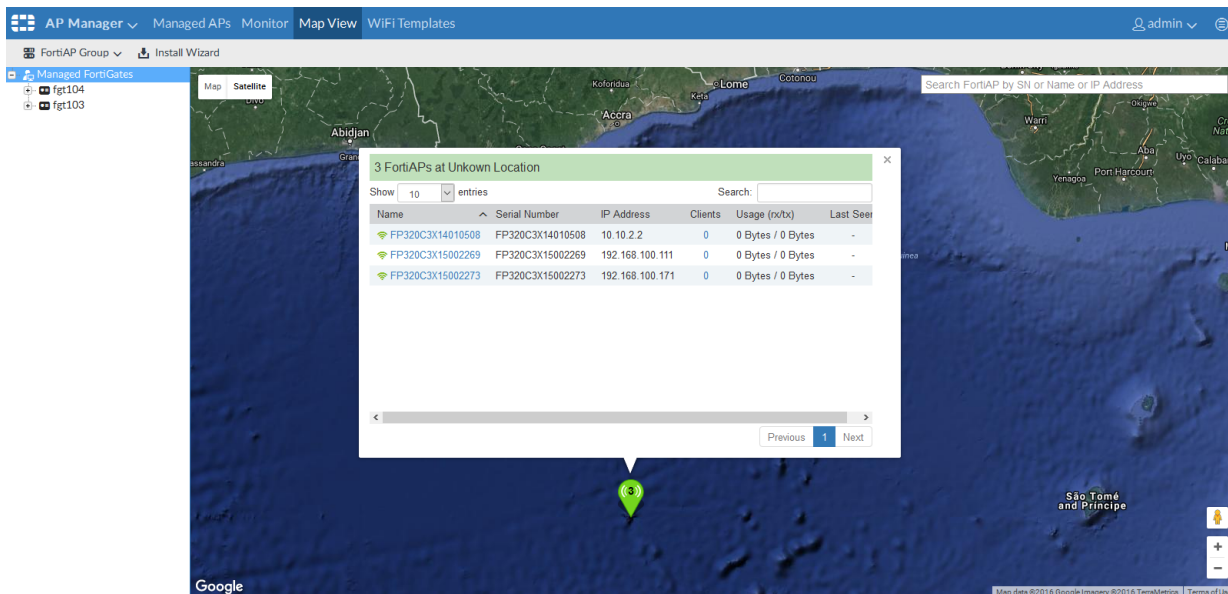
Widgets can be moved by clicking and dragging their title bar into different locations on the screen. The information in the widgets can be refreshed by clicking the refresh icon in the widget title bar. Widgets with tables can be sorted by any column by clicking the column name.

The following widgets are shown:

Widget	Description
AP Status	<p>Displays a bar graph of:</p> <ul style="list-style-type: none"> • <i>Uptime > 24 hours</i>: The number of APs that have been up for over 24 hours. • <i>Rebooted within 24 hours</i>: the number of APs that have been rebooted within the past 24 hours. • <i>Down/Missing</i>: Down or missing APs. <p>Select a specific column to view a table of the APs represented in that column, along with other relevant information, such as the APs' IP address, and the time of its last reboot.</p> <p>Select the name of a column in the legend to add or remove it from the graph.</p> <p>This widget is only available when the <i>All FortiAPs</i> group is selected in the tree menu.</p>
Client Count Over Time	<p>A graph of the number of connected clients over the specified time period: 1 hour, 1 day, or 30 days.</p> <p>This widget is only available when the <i>All FortiAPs</i> group is selected in the tree menu.</p>
Top Client Count Per-AP (2.4 GHz or 5 GHz Band)	<p>Lists the number of clients in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and bandwidth of the AP.</p>
Top Wireless Interference (2.4 GHz or 5 GHz Band)	<p>Lists the number of interfering APs in the 2.4GHz and 5GHz band for each FortiAP. Also includes columns for the channel and the number of MAC Errors for each AP.</p>
Login Failures Information	<p>Lists the time of a log in failure, the SSID involved, the Host Name/MAC, and the User Name.</p>

Map View

The Map View pane shows all of the FortiGate controllers on an interactive world map (Google Maps). Each FortiGate is designated by a map pin in its geographic location on the map. The number of APs connected to the FortiGate is listed in the pin.



Clicking on a map pin opens a list of the APs connected to that FortiGate. Clicking on the name of an AP from the list will zoom the map into that location and provide further information about the AP, including the serial number, IP address, number of clients, usage, and the last time the AP was seen if it is offline.

Click on the number of clients to open the *View WiFi Clients* window (see [Connected clients on page 320](#)). Click on the AP's serial number to open the *Config FortiAP* window, where you can edit the AP settings (see [Managing APs on page 313](#)).

WiFi templates

The *WiFi Templates* pane allows you to create and manage AP profiles, SSIDs, and Wireless Intrusion Detection System (WIDS) profiles that can be assigned to managed FortiAP devices.

In per-device mode, templates are not shared between devices.



Settings may vary for different ADOM versions.

AP profiles

AP profiles define radio settings for FortiAP models. The profile specifies details such as the operating mode of the device, SSIDs, and transmit power. Custom AP profiles can be created as needed for new devices.

To view AP profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Templates*, and select *AP Profile* in the tree menu.

Name	Platform	Radio 1	Radio 2	Comment
<input checked="" type="checkbox"/> 11n-only	FortiWiFi local radio.	802.11bgn_2.4G		
<input type="checkbox"/> FAP112B-default	FAP112B	802.11bgn_2.4G		
<input type="checkbox"/> FAP112D-default	FAP112D	802.11bgn_2.4G		
<input type="checkbox"/> FAP11C-default	FAP11C	802.11bgn_2.4G		
<input type="checkbox"/> FAP14C-default	FAP14C	802.11bgn_2.4G		
<input type="checkbox"/> FAP210B-default	FAP210B	802.11bgn_2.4G		
<input type="checkbox"/> FAP21D-default	FAP21D	802.11bgn_2.4G		
<input type="checkbox"/> FAP220B-default	FAP220B/221B	802.11an_5G	802.11bgn_2.4G	
<input type="checkbox"/> FAP221C-default	FAP221C	802.11bgn_2.4G	802.11ac	
<input type="checkbox"/> FAP222B-default	FAP222B	802.11bgn_2.4G	802.11an_5G	
<input type="checkbox"/> FAP222C-default	FAP222C	802.11bgn_2.4G	802.11ac	
<input type="checkbox"/> FAP223B-default	FAP223B	802.11an_5G	802.11bgn_2.4G	
<input type="checkbox"/> FAP223C-default	FAP223C	802.11bgn_2.4G	802.11ac	

The following options are available in the toolbar and right-click menu:

Create New	Create a new AP profile.
Edit	Edit the selected AP profile.
Delete	Delete the selected AP profile.
Clone	Clone the selected AP profile.
Import	Import AP profiles from a connected FortiGate (toolbar only).

To create custom AP profiles:

1. On the *AP Profile* pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New AP Profile* windows opens.

Create New AP Profile

Name

Comments

Write a comment

0/255

Platform

FAP220B/221B

AP Country Code

US (UNITED STATES)

AP Login Password

☐ Set
☒ Leave Unchanged
☐ Set Empty

Split Tunneling Subnet(s)

Radio 1

Operation Mode

☐ Disabled
☒ Access Point
☐ Dedicated Monitor

WIDS Profile

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff
☐ AP Handoff

Band

802.11n/a radio at 5GHz band.

Short Guard Interval

☐

Select Channel Width

20MHZ

Channel

☒ 36
☒ 40
☒ 44
☒ 48
☒ 52*
☒ 56*
☒ 60*
☒ 64*
☒ 100*
☒ 104*
☒ 108*
☒ 112*
☒ 116*
☒ 120*
☒ 124*
☒ 128*
☒ 132*
☒ 136*
☒ 140*

Auto TX Power Control

☒ Disable
☐ Enable

TX Power

100%

SSID

Available

Selected

Radio 2

Operation Mode

☐ Disabled
☐ Access Point
☒ Dedicated Monitor

WIDS Profile

Location Based Services

FortiPresence

Project name

fortipresence

Password

••••••••

FortiPresence server IP

FortiPresence server port

3000

Report rogue APs

☐

Report unassociated clients

☒

Report transmit frequency (in seconds)

30

☐ Ekahau blink
☐ AeroScout
☐ Locate WiFi clients when not connected

[Advanced Options](#)

OK

Cancel

2. Enter the following information:

Name	Type a name for the profile.
Comment	Optionally, enter comments.
Platform	Select the platform that the profile will apply to from the dropdown list.
AP Country Code	Select the AP country code from the dropdown list.
AP Login Password	Set, leave unchanged, or empty the AP login password.
Split Tunneling Subnet(s)	Enter the split tunneling subnet(s).
Radio 1 & 2	Configure the radio settings. The Radio 2 settings will only appear if the selected platform has two radios.
Operation Mode	Select the radio operation mode: <ul style="list-style-type: none"> <i>Disabled</i>: The radio is disabled. No further radio settings are available. <i>Access Point</i>: The device is an access point. <i>Dedicated Monitor</i>: The device is a dedicated monitor. Only the <i>WIDS Profile</i> settings is available.

WIDS Profile	Select a WIDS profile from the dropdown list. See WIDS profiles on page 336 .
Radio Resource Provision	Select to enable radio resource provisioning. This feature measures utilization and interference on the available channels and selects the clearest channel at each access point.
Client Load Balance	Select the client load balancing methods to use: <i>Frequency Handoff</i> and/or <i>AP Handoff</i> .
Band	Select the wireless protocol from the dropdown list. The available bands depend on the selected platform. In two radio devices, both radios cannot play in the same band.
Short Guard Interval	Select to enable the short guard interval. This option is only available for 2.4GHz 802.11n/g/b, and 5GHz 802.11n bands.
Select Channel Width	Select 20MHz or 40MHz channel width. This option is only available for 5GHz 802.11n bands.
Channel	Select the channel or channels to include. The available channels depend on the selected platform and band.
Auto TX Power Control	Optionally, enable automatic adjustment of transmit power, then specify the minimum and maximum power levels, dBm.
TX Power	If <i>Auto TX Power Control</i> is disabled, enter the TX power in the form of the percentage of the total available power.
SSID	Choose the SSIDs that APs using this profile will carry.
FortiPresence	
Mode	Select the FortiPresence mode: <ul style="list-style-type: none"> • <i>Disable</i> • <i>Foreign channels only</i> • <i>Foreign and home channels</i>
Project name	The FortiPresence project name.
Password	FortiPresence secret password.
FortiPresence server IP	FortiPresence server IP address.
FortiPresence server port	FortiPresence server UDP listening port (default = 3000).
Report rogue APs	Enable/disable FortiPresence reporting of Rogue APs.
Report unassociated clients	Enable/disable FortiPresence reporting of unassociated devices.

Report transmit frequency (in seconds)	FortiPresence report transmit frequency, in seconds (5 - 65535, default = 30).
Ekahau blink	Enable/disable Ekahau blink location based services.
RTLS controller server IP	Enter the realtime location services (RTLS) controller server IP address.
RTLS controller server port	Enter the RTLS controller server port (default = 8569).
Ekahau tag MAC address	Enter the Ekahau tag MAC address.
AeroScout	Enable/disable AeroScout location based services.
AeroScout server IP	Enter the AeroScout server IP address.
AeroScout server port	Enter the AeroScout server port.
MU mode dilution factor	Enter the MU mode dilution factor (default = 20).
MU mode dilution timeout	Enter the MU mode dilution timeout (default = 5).
Locate WiFi clients when not connected	Enable/disable locating WiFi client when they are not connected.

Advanced Options

Configure advanced options for the SSID.

- *allowaccess*: Allow management access to the managed AP via *telnet*, *http*, *https*, and/or *ssh*.
- *dtls-in-kernal*: Enable/disable data channel DTLS in kernel.
- *dtls-policy*: Select the WTP data channel DTLS policy: *clear-text*, *dtls-enabled*, and/or *ipsec-vpn*.
- *handoff-roaming*: Enable/disable handoff when a client is roaming.
- *handoff-rssi*: Enter the minimum RSSI handoff value.
- *handoff-sta-thresh*: Enter the threshold value for AP handoff.
- *ip-fragment-preventing*: Prevent IP fragmentation for CAPWAP tunneled control and data packets. Select *tcp-mss-adjust* and/or *icmp-unreachable*.
- *led-state*: Enable/disable use of LEDs on WTP.
- *lldp*: Enable/disable LLDP.
- *login-passwd*: Enter the log in password of the managed AP.
- *login-passwd-change*: Select whether or not to allow the log in password to be changed, or to reset to the factory default setting.
- *max-clients*: Enter the maximum number of STAs supported by the WTP.
- *split-tunneling-acl-local-ap-subnet*: Enable/disable split tunneling ACL local AP subnet.
- *tun-mtu-downlink*: Enter the downlink tunnel MTU.
- *tun-mtu-uplink*: Enter the uplink tunnel MTU.
- *wan-port-mode*: Set the WAN port mode: *wan-only* or *wan-lan*.

3. Click **OK** to create the new AP profile.

To edit a custom AP profile:

1. Either double-click a profile name, right-click a profile name and select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit AP Profile* pane opens.
2. Edit the settings as required. The profile name cannot be edited.
3. Click **OK** to apply your changes.

To delete custom AP profiles:

1. Select the AP profile or profiles that will be deleted. Default profiles cannot be deleted.
2. Either select *Delete* from the toolbar, or right-click and select *Delete*.
3. Click **OK** in the confirmation dialog box to delete the profile.

To clone a custom AP profile:

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone AP Profile* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click **OK** to clone the profile.

To import a AP profile:

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

SSIDs

To view SSIDs and SSID groups, go to *AP Manager > WiFi Templates*, and select *SSID* in the tree menu.

The following options are available in the toolbar and right-click menu:

Create New	Create a new SSID or SSID group.
Edit	Edit the selected SSID or group.
Delete	Delete the selected SSID or group.
Clone	Clone the selected SSID or group.
Import	Import SSIDs from a connected FortiGate (toolbar only).

When creating a new SSID, the available options will change depending on the selected traffic mode: *Tunnel to Wireless Controller*, *Local bridge with FortiAP's Interface*, or *Mesh Downlink*.

To create a new SSID (Tunnel to Wireless Controller):

1. On the SSID pane, click *Create New > SSID* in the toolbar, or select it from the right-click menu. The *Create New SSID Profile* windows opens.

Create New SSID Profile

Name

Traffic Mode Tunnel to Wireless Controller

Common Interface Settings ☒

IP/Netmask

IPv6 Address

Administrative Access ☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access
☐ SSH ☐ SNMP ☐ TELNET ☐ Auto IPsec Request ☐ FCT-Access

IPv6 Administrative Access ☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access
☐ SSH ☐ SNMP ☐ TELNET
☐ CAPWAP

Enable DHCP ☐

WiFi Settings

SSID

Security Mode WPA/WPA2-PERSONAL

Pre-shared Key

Schedule ☒ Click to add...

Block Intra-SSID Traffic ☐

Split Tunneling ☐

Maximum Clients ☐ Limit Concurrent WiFi Clients

Optional VLAN ID

VLAN Pool ☒ Click to add...

Device Detection ☒ Add New Devices to Vulnerability Scan List ☐

Advanced Options

2. Enter the following information, then click **OK** to create the new tunnel to wireless controller SSID:

Name	Type a name for the SSID.
Traffic Mode	Select <i>Tunnel to Wireless Controller</i> from the dropdown list.
Common Interface Settings	Select to apply common interface settings for this SSID on all FortiAPs to which this template is applied. Common settings include IP addresses, administrative access, and DHCP settings.
IP/Netmask	Type the IP address and netmask.
IPv6 Address	Type the IPv6 address.
Administrative Access	Select the allowed administrative service protocols from: <i>HTTPS</i> , <i>HTTP</i> , <i>PING</i> , <i>FMG-Access</i> , <i>SSH</i> , <i>SNMP</i> , <i>TELNET</i> , <i>Auto IPsec Request</i> , and <i>FCT-Access</i> .
IPv6 Administrative Access	Select the allowed IPv6 administrative service protocols from: <i>HTTPS</i> , <i>HTTP</i> , <i>PING</i> , <i>FMG-Access</i> , <i>SSH</i> , <i>SNMP</i> , <i>TELNET</i> , and <i>CAPWAP</i> .
Enable DHCP	Select to enable and configure DHCP. This option is only available if <i>Common Interface Settings</i> is enabled. Note: If <i>Mode</i> is <i>Relay</i> , only the <i>DHCP Server IP</i> and <i>Type</i> settings are available.
Address Range	Enter the DHCP address range. This option is only available when <i>Mode</i> is set to <i>Server</i> .
Netmask	Enter the netmask. This option is only available when <i>Mode</i> is set to <i>Server</i> .
Default Gateway	Select <i>Same As Interface IP</i> if the default gateway is the same as the interface IP, or select <i>Specify</i> and type a new gateway IP address. This option is only available when <i>Mode</i> is set to <i>Server</i> .
DNS Server	Select <i>Same As System DNS</i> if the DNS server is the same as the system DNS, or select <i>Specify</i> and type a DNS server address. This option is only available when <i>Mode</i> is set to <i>Server</i> .
Mode	Select <i>Server</i> or <i>Relay</i> .
DHCP Server IP	Enter the DHCP server IP address. This option is only available if <i>Mode</i> is set to <i>Relay</i> .
MAC Address Access Control List	The MAC address control list allows you to view the MAC addresses and their actions. It includes a default entry for unknown MAC addresses. <ul style="list-style-type: none"> Click <i>Create New</i> to create a new IP MAC binding. Select an address then click <i>Edit</i> to edit the MAC address. Select an address or addresses then click <i>Delete</i> to delete the selected items. The unknown MAC address cannot be deleted. This option is only available if <i>Mode</i> is set to <i>Server</i> .

Type	Select <i>Regular</i> or <i>IPsec</i> .																
Lease Time	Enter the lease time, in seconds.																
WiFi Settings																	
SSID	Type the wireless service set identifier (SSID), or network name, for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.																
Security Mode	<p>Select a security mode. The options will vary depending on the selected traffic mode:</p> <table> <tr> <td><i>none</i></td><td><i>Captive Portal</i></td></tr> <tr> <td><i>WPA_PSK</i></td><td><i>OPEN</i></td></tr> <tr> <td><i>WPA_RADIUS</i></td><td><i>WPA2-ONLY-PERSONAL</i></td></tr> <tr> <td><i>WPA</i></td><td><i>WPA2-ONLY-ENTERPRISE</i></td></tr> <tr> <td><i>WPA2</i></td><td><i>WPA/WPA2 Personal with Captive Portal</i></td></tr> <tr> <td><i>WPA2_AUTO</i></td><td><i>WPA2 Personal with Captive Portal</i></td></tr> <tr> <td><i>WPA/WPA2-PERSONAL</i></td><td></td></tr> <tr> <td><i>WPA/WPA2-ENTERPRISE</i></td><td></td></tr> </table>	<i>none</i>	<i>Captive Portal</i>	<i>WPA_PSK</i>	<i>OPEN</i>	<i>WPA_RADIUS</i>	<i>WPA2-ONLY-PERSONAL</i>	<i>WPA</i>	<i>WPA2-ONLY-ENTERPRISE</i>	<i>WPA2</i>	<i>WPA/WPA2 Personal with Captive Portal</i>	<i>WPA2_AUTO</i>	<i>WPA2 Personal with Captive Portal</i>	<i>WPA/WPA2-PERSONAL</i>		<i>WPA/WPA2-ENTERPRISE</i>	
<i>none</i>	<i>Captive Portal</i>																
<i>WPA_PSK</i>	<i>OPEN</i>																
<i>WPA_RADIUS</i>	<i>WPA2-ONLY-PERSONAL</i>																
<i>WPA</i>	<i>WPA2-ONLY-ENTERPRISE</i>																
<i>WPA2</i>	<i>WPA/WPA2 Personal with Captive Portal</i>																
<i>WPA2_AUTO</i>	<i>WPA2 Personal with Captive Portal</i>																
<i>WPA/WPA2-PERSONAL</i>																	
<i>WPA/WPA2-ENTERPRISE</i>																	
Pre-shared Key	<p>Enter the pre-shared key for the SSID.</p> <p>This option is only available when the security mode includes WPA or WPA2 personal.</p>																
Authentication	<p>Select the authentication method for the SSID, either <i>Local</i> or <i>RADIUS Server</i>, then select the requisite server or group from the dropdown list.</p> <p>This option is only available when the security mode includes WPA2 enterprise.</p>																
Portal Type	<p>Select the portal type, one of: <i>Authentication</i>, <i>Disclaimer + Authentication</i>, <i>Disclaimer Only</i>, or <i>Email Collection</i>.</p> <p>This option is only available when the security mode includes captive portal.</p>																
Authentication Portal	<p>Select <i>Local</i> or <i>External</i>. If <i>External</i> is selected, enter the URL of the portal.</p> <p>This option is only available when the portal type includes authentication.</p>																
User Groups	<p>Select the user group to add from the dropdown list. Select the plus symbol to add multiple groups.</p> <p>This option is only available when the portal type includes authentication.</p>																
Exempt Sources	<p>Select exempt sources to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>																
Exempt Devices	<p>Select exempt devices to add from the dropdown list.</p> <p>This option is only available when the portal type includes authentication.</p>																

Exempt Destinations	Select exempt destinations to add from the dropdown list. This option is only available when the portal type includes authentication.
Exempt Services	Select exempt services to add from the dropdown list. This option is only available when the portal type includes authentication.
Customize Portal Messages	Select to allow for customized portal messages. Portal messages cannot be customized until after the interface has been created. This option is only available when the portal type includes disclaimer or email collection.
Redirect after Captive Portal	Select <i>Original Request</i> or <i>Specific URL</i> . If <i>Specific URL</i> is selected, enter the redirect URL. This option is only available when the security mode includes captive portal.
Schedule	Select a schedule to control the availability of the SSID. For information on creating a schedule object, see Create a new object on page 262 .
Block Intra-SSID Traffic	Select to block intra-SSID traffic.
Split Tunneling	Select to enable split tunneling.
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients.
Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
VLAN Pool	Select AP groups to add to the VLAN pool
Device Detection	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.
Advanced Options	
broadcast-ssid	Enable/disable SSID broadcast in the beacon.
encrypt	Select the data encryption protocol: <i>TKIP</i> , <i>AES</i> , or <i>TKIP-AES</i> .

To create a new SSID (Local bridge with FortiAP's Interface):

1. On the SSID pane, click *Create New > SSID* in the toolbar.
2. Enter the following information, then click *OK* to create the new local bridge SSID:

Name	Type a name for the SSID.
Traffic Mode	Select <i>Local bridge with FortiAP's Interface</i> from the dropdown list.

WiFi Settings	
SSID	Type the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
Security Mode	<p>Select a security mode. The options are:</p> <div> <div>WPA/WPA2-PERSONAL</div> <div>WPA/WPA2-ENTERPRISE</div> <div>OPEN</div> <div>WPA-ONLY-PERSONAL</div> <div>WPA-ONLY-ENTERPRISE</div> <div>WPA2-ONLY-PERSONAL</div> <div>WPA2-ONLY-ENTERPRISE</div> </div>
Pre-shared Key	<p>Enter the pre-shared key for the SSID.</p> <p>This option is only available when the security mode includes WPA or WPA2 personal.</p>
Authentication	<p>Select the authentication method for the SSID, either <i>Local</i> or <i>RADIUS Server</i>, then select the requisite server or group from the dropdown list.</p> <p>This option is only available when the security mode is includes WPA or WPA2 enterprise.</p>
Schedule	Select a schedule to control the availability of the SSID. For information on creating a schedule object, see Create a new object on page 262 .
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
Optional VLAN ID	Select the VLAN ID in the text field using the arrow keys. Select 0 if VLANs are not used.
VLAN Pool	Select AP groups to add to the VLAN pool
Device Detection	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.
Advanced Options	
broadcast-ssid	Enable/disable SSID broadcast in the beacon.
encrypt	Select the data encryption protocol: <i>TKIP</i> , <i>AES</i> , or <i>TKIP-AES</i> .

To create a SSID (Mesh Downlink):

1. On the SSID pane, click *Create New > SSID* in the toolbar.
2. Enter the following information, then click *OK* to create the SSID:

Name	Type a name for the SSID.
Traffic Mode	Select <i>Mesh Downlink</i> from the dropdown list.

WiFi Settings	
SSID	Type the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name.
Security Mode	Select a security mode. The options are: <div> <div>WPA/WPA2-PERSONAL</div> <div>WPA-ONLY-PERSONAL</div> <div>OPEN</div> <div>WPA2-ONLY-PERSONAL</div> </div>
Pre-shared Key	Enter the pre-shared key for the SSID.
Schedule	Select a schedule to control the availability of the SSID. For information on creating a schedule object, see Create a new object on page 262 .
Maximum Clients	Select to limit the concurrent WiFi clients that can connect to the SSID. If selected, type the desired maximum number of clients. Type 0 for no limit.
Device Detection	Select to detect and identify devices connecting to the SSID.
Add New Devices to Vulnerability Scan List	Select to add new devices to the vulnerability scan list.
Advanced Options	
broadcast-ssid	Enable/disable SSID broadcast in the beacon.
encrypt	Select the data encryption protocol: <i>TKIP</i> , <i>AES</i> , or <i>TKIP-AES</i> .

3. Click *OK* to create the SSID.

To create a new SSID group:

1. On the SSID pane, click *Create New > SSID Group* in the toolbar. The *Create New SSID Group* window opens.
2. Enter a name for the group in the *Name* field.
3. Optionally, enter a brief description of the group in the *Comment* box.
4. Optionally, add SSIDs to the group in the *Members* field.
5. Click *OK* to create the SSID group.

To edit an SSID or groups:

1. Either double-click on an SSID, select as SSID and then click *Edit* in the toolbar, or right-click then select *Edit* from the menu. The *Edit SSID* or *Edit SSID Group* window opens.
2. Edit the settings as required. The SSID name and traffic mode cannot be edited.
3. Click *OK* to apply your changes.

To delete SSIDs or groups:

1. Select the SSIDs and groups that you would like to delete.
2. Either click *Delete* in the toolbar, or right-click and select *Delete*.

3. Click *OK* in the confirmation dialog box to delete the selected SSIDs and groups.

Deleting a group does not delete the SSIDs that are in the group.

To clone an SSID or group:

1. Either select an SSID or group and click *Clone* in the toolbar, or right-click on the SSID or group name, and select *Clone*. The *Clone SSID* or *Clone SSID Group* dialog box opens.
2. Edit the settings as required. An SSID's traffic mode cannot be edited.
3. Click *OK* to clone the SSID.

To import an SSID:

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the SSID or SSIDs to be imported from the *Profile* dropdown list.
4. Click *OK* to import the SSID or SSIDs.

WIDS profiles

The WIDS monitors wireless traffic for a wide range of security threats by detecting and reporting on possible intrusion attempts. When an attack is detected, a log message is recorded.

To view WIDS profiles, ensure that you are in the correct ADOM, go to *AP Manager > WiFi Templates*, and select *WIDS Profile* in the tree menu.

The following options are available in the toolbar and right-click menu:

Create New	Create a new WIDS profile.
Edit	Edit the selected WIDS profile.
Delete	Delete the selected WIDS profile.
Clone	Clone the selected WIDS profile.
Import	Import WIDS profiles from a connected FortiGate (toolbar only).

To create a new WIDS profile:

1. On the WIDS Profile pane, click *Create New* in the toolbar, or select it from the right-click menu. The *Create New WIDS Profile* window opens.

Create New WIDS Profile

Name

Comments

☐ Enable Rogue AP Detection

Intrusion Type	Status	Threshold (Seconds)	Interval (Seconds)
Asleep Attack	<input type="checkbox"/>		
Association Frame Flooding	<input type="checkbox"/>	30 (1-100)	10 (5-120)
Authentication Frame Flooding	<input type="checkbox"/>	30 (1-100)	10 (5-120)
Broadcasting De-authentication	<input type="checkbox"/>		
EAPOL-FAIL Flooding (to AP)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
EAPOL-LOGOFF Flooding (to AP)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
EAPOL-START Flooding (to AP)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
EAPOL-SUCC Flooding (to AP)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
invalid MAC OU	<input type="checkbox"/>		
Long Duration Attack	<input type="checkbox"/>	8200 (1000-32767) microsecond	
Null SSID Probe Response	<input type="checkbox"/>		
Premature EAPOL-FAIL Flooding (to Client)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
Premature EAPOL-SUCC Flooding (to Client)	<input type="checkbox"/>	10 (2-100)	1 (1-3600)
Spoofed De-authentication	<input type="checkbox"/>		
Weak WEP IV (Initialization Vector)	<input type="checkbox"/>		
Wireless Bridge	<input type="checkbox"/>		

OK Cancel

2. Enter the following information:

Name	Enter a name for the profile.
Comments	Optionally, enter comments.
Enable Rogue AP Detection	Select to enable rogue AP detection.
Background Scan Every Second(s)	Enter the number of seconds between background scans.
Disable Background Scan During Specified Time	Select to disables background scanning during the specified time. Specify the days of week, and the start and end times.
Enable Passive Scan Mode	Select to enable passive scan mode.
Enable On-Wire Rogue AP Detection	Select to enable on-wire rogue AP detection. When enabled you can select to auto suppress rogue APs in foreground scan.
Intrusion Type	The intrusion types that can be detected.
Status	Select to enable the intrusion type.
Threshold	If applicable, enter a threshold for reporting the intrusion, in seconds except where specified.
Interval (sec)	If applicable, enter the interval for reporting the intrusion, in seconds.

3. Click *OK* to create the new WIDS profile.

Intrusion types

Intrusion Type	Description
Asleep Attack	ASLEAP is a tool used to perform attacks against LEAP authentication.
Association Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Authentication Frame Flooding	A Denial of Service attack using association requests. The default detection threshold is 30 requests in 10 seconds.
Broadcasting De-authentication	This is a type of Denial of Service attack. A flood of spoofed de-authentication frames forces wireless clients to de-authenticate, then re-authenticate with their AP.
EAPOL Packet Flooding (to AP)	<p>Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the AP with these packets can be a denial of service attack.</p> <p>Several types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> • EAPOL-FAIL • EAPOL-LOGOFF • EAPOL-START • EAPOL-SUCC
Invalid MAC OU	Some attackers use randomly-generated MAC addresses. The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE. Invalid OUIs are logged.
Long Duration Attack	To share radio bandwidth, WiFi devices reserve channels for brief periods of time. Excessively long reservation periods can be used as a denial of service attack. You can set a threshold between 1000 and 32 767 microseconds. The default is 8200.
Null SSID Probe Response	When a wireless client sends out a probe request, the attacker sends a response with a null SSID. This causes many wireless cards and devices to stop responding.
Premature EAPOL Packet Flooding (to client)	<p>Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication. Flooding the client with these packets can be a denial of service attack.</p> <p>Two types of EAPOL packets can be detected:</p> <ul style="list-style-type: none"> • EAPOL-FAIL • EAPOL-SUCC
Spoofed De-authentication	Spoofed de-authentication frames form the basis for most denial of service attacks.

Intrusion Type	Description
Weak WEP IV Detection	A primary means of cracking WEP keys is by capturing 802.11 frames over an extended period of time and searching for patterns of WEP initialization vectors (IVs) that are known to be weak. WIDS detects known weak WEP IVs in on-air traffic.
Wireless Bridge	WiFi frames with both the FromDS and ToDS fields set indicate a wireless bridge. This will also detect a wireless bridge that you intentionally configured in your network.

To edit a WIDS profile:

1. Either double-click on a profile name, select a profile and then click *Edit* in the toolbar, or right-click on the name then select *Edit* from the menu. The *Edit WIDS* window opens.
2. Edit the settings as required.
3. Click *OK* to apply your changes.

To delete WIDS profiles:

1. Select the profile or profiles that will be deleted from the profile list.
2. Either click *Delete* from the toolbar, or right-click then select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the profile or profiles.

To clone a WIDS profile:

1. Either select a profile and click *Clone* in the toolbar, or right-click a profile and select *Clone*. The *Clone WIDS* pane opens.
2. Edit the name of the profile, then edit the remaining settings as required.
3. Click *OK* to clone the profile.

To import a WIDS profile:

1. Click *Import* in the toolbar. The *Import* dialog box opens.
2. Select a FortiGate from the dropdown list. The list will include all of the devices in the current ADOM.
3. Select the profile or profiles to be imported from the dropdown list.
4. Click *OK* to import the profile or profiles.

FortiClient Manager

The *FortiClient Manager* pane enables you to centrally manage FortiClient profiles for multiple FortiGate devices and monitor FortiClient endpoints that are connected to FortiGate devices.

Endpoint control ensures that workstation computers (endpoints) and other network devices meet security requirements. Otherwise they are not permitted access. Endpoint control enforces the use of FortiClient Endpoint Security and pushes a FortiClient profile to the FortiClient application.

For information about FortiClient, see the *FortiClient Administration Guide*.



Additional configuration options and shortcuts are available using the right-click menu. Right-click on different parts of the navigation panes in the GUI to access these menus.

The *FortiClient Manager* pane includes the following tabs in the blue banner:

FortiTelemetry	View managed FortiGate devices with central FortiClient management enabled. You can enable or disable FortiTelemetry for interfaces, enable or disable FortiClient enforcement on interfaces, and assign FortiClient profile packages to devices.
Monitor	Monitor FortiClient endpoints by compliance status or interface. You can perform the following actions on FortiClient endpoints: block, unblock, quarantine, release quarantine, and unregister. You can also exempt non-compliant FortiClient endpoints from compliance rules.
FortiClient profiles	View and create profile packages and FortiClient profiles. You can also import FortiClient profiles from FortiGate devices.

Centralized FortiClient management is enabled by default. You use the *FortiClient Manager* pane to enable FortiTelemetry and FortiClient enforcement on FortiGate interfaces as well as create and assign FortiClient profile packages to one or more FortiGate devices or VDOMs. Profile packages are installed to devices when you install configurations to the devices.

The following steps provide an overview of using centralized FortiClient management to configure, assign, and install FortiClient profiles:

To create and assign FortiClient profile packages:

1. Create a FortiClient profile package. See [Creating FortiClient profile packages on page 347](#).
2. Select the profile package, and create one or more FortiClient profiles. See [Creating FortiClient profiles on page 348](#).
3. Enable FortiTelemetry on FortiGate interfaces. See [Enabling FortiTelemetry on interfaces on page 342](#).
4. Enable FortiClient enforcement on FortiGate interfaces. See [Enabling endpoint control on interfaces on page 343](#).
5. Assign profile packages to FortiGate interfaces. See [Assigning profile packages on page 352](#).

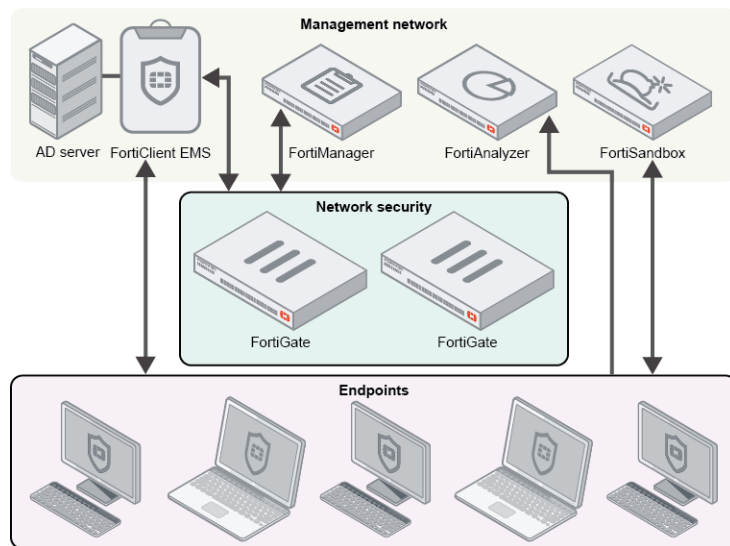
To install configuration changes to devices:

1. On the *FortiClient Manager* > *FortiClient Profiles* pane, click *Install Wizard*.
2. Follow the prompts in the wizard. See [Using the Install Wizard to install policy packages and device settings on page 134](#).

How FortiManager fits into endpoint compliance

The FortiClient settings available in FortiManager are intended to complement FortiClient support that is available with FortiClient EMS and FortiGate. Each product performs specific functions:

- FortiClient EMS is used to deploy FortiClient (Windows) endpoints and FortiClient profiles, and the endpoints can connect FortiClient Telemetry to FortiGate or to FortiClient EMS. You can import FortiClient profiles from FortiGate devices to FortiClient EMS, and use FortiClient EMS to deploy the profiles. Alternately, you can use FortiClient EMS to create and deploy profiles. When FortiClient endpoints connect FortiClient Telemetry to EMS, you can use FortiClient EMS to monitor FortiClient endpoints.
- FortiManager provides central FortiClient management for FortiGate devices that are managed by FortiManager. In FortiManager, you can create one or more FortiClient profiles that you can assign to multiple FortiGate devices. You can also import FortiClient profiles from one FortiGate device and assign the FortiClient profile to other FortiGate devices. When FortiClient endpoints are registered to managed FortiGate devices, you can use FortiManager to monitor FortiClient endpoints from multiple FortiGate devices.
- FortiGate provides compliance rules for network access control. FortiGate devices enforce network compliance for connected FortiClient endpoints. FortiGate devices communicate between FortiClient endpoints and FortiManager.



FortiTelemetry

On the *FortiClient Manager* > *FortiTelemetry* pane, you can enable and disable FortiTelemetry and FortiClient enforcement on FortiGate interfaces to use for FortiClient communication. You can also assign FortiClient profile

packages to FortiGate devices.

After you make configuration changes, install the changes to the device. See [Installing to devices on page 134](#).

Viewing devices

The *FortiClient Manager > FortiTelemetry* pane displays FortiGate devices with central FortiClient management enabled.

To view devices:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
3. Select a device.

The following options are available in the toolbar for the selected device:

Add Interface	Click to enable FortiTelemetry on interfaces for the selected device to use for FortiClient communication.
Remove Interface	Click to disable FortiTelemetry on the selected interface.
Assign Profile	Click to assign a FortiClient profile package to the FortiGate.

The following information is displayed in the content pane for the selected device:

Virtual Domain	Displays the name of the virtual domain for the selected FortiGate device if applicable.
Interface	Displays the interfaces with FortiTelemetry enabled for the FortiGate device. The interfaces are used for FortiClient communication, and FortiClient endpoints use the interface to connect or register to FortiGate.
IP	Displays the IP address for the interface.
Enforce FortiClient	Displays whether FortiClient is enforced on the interface. A green checkmark indicates FortiClient is enforced. An x in a circle indicates that FortiClient is not enforced.
Profile Package	Displays the name of the FortiClient profile package that is assigned to the FortiGate interface.

Enabling FortiTelemetry on interfaces

When you add an interface on the *FortiClient Manager > FortiTelemetry* pane, you are enabling FortiTelemetry for the interface, and the interface is used for connection and communication with FortiClient endpoints.

When you remove an interface on the *FortiClient Manager > FortiTelemetry* pane, you are disabling FortiTelemetry for the interface.

To enable FortiTelemetry on interfaces:

1. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
2. Select a FortiGate device, and click *Add Interface*.
3. Select one or more interfaces to use for FortiClient communication, and click *OK*. The selected interfaces are displayed in the *Interface* column, and FortiTelemetry is enabled for the interfaces.

Enabling endpoint control on interfaces

When you enable FortiClient enforcement on an interface, you are enabling endpoint control, and all FortiClient endpoints using the interface are required to adhere to the FortiGate compliance rules that are specified in the profile that is applied to the endpoint.

When you disable FortiClient enforcement on an interface, you are disabling endpoint control, and FortiClient endpoints are not required to adhere to FortiGate compliance rules.

To enable FortiClient enforcement on interfaces:

1. Go to *FortiClient Manager > FortiTelemetry*. The list of FortiGate devices is displayed in the tree menu.
2. Click a FortiGate device.
3. Right-click an interface, and select *Enable Enforce FortiClient*.

You can disable FortiClient enforcement for the interface by selecting *Disable Enforce FortiClient*.

Assigning FortiClient profile packages to devices

You can use the *FortiClient Manager > FortiTelemetry* pane to assign FortiClient profile packages to interfaces for FortiGate devices, and you can use the *Install Wizard* to install profile packages to FortiGate devices when you install a configuration to the FortiGate device.

To assign FortiClient profile packages:

1. In the left pane, select a device.
2. In the content pane, click *Assign Profile*. The *Assign Profile* dialog box is displayed.
3. Select a profile package, and click *OK*. The selected profile package is assigned to the added interface(s).
4. Install the configuration changes to the FortiGate device.

Monitor

On the *FortiClient Manager > Monitor* pane, you can monitor FortiClient endpoints that are registered to FortiGate devices.

Monitoring FortiClient endpoints

The list of FortiClient endpoints updates automatically when new endpoints are registered to the FortiGate device. You can also click *Refresh* to update the list of FortiClient endpoints.

To monitor FortiClient endpoints:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiClient Manager > Monitor*.
3. In the tree menu, select a FortiGate device.

The following buttons are available on the toolbar for the selected device:

Refresh	Click to refresh the list of FortiClient endpoints for the selected device.
Action	Click to select one of the following actions for the selected FortiClient endpoint: <ul style="list-style-type: none"> • Block • Unblock • Quarantine • Release Quarantine • Unregister
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.
By Interface	Click to organize the display of FortiClient endpoints by the undetected interfaces and interface name. In the <i>Device</i> column, click <i>Undetected</i> or the interface name to hide and display its list of FortiClient endpoints.
By Compliance Status	Click to organize the display of FortiClient endpoints by the following compliance statuses: <i>Noncompliant</i> and <i>Exempt</i> . In the <i>Device</i> column, click <i>Noncompliant</i> or <i>Exempt</i> to hide and display its list of FortiClient endpoints.

The following default columns of information are available for the selected device:

Device	Displays the name of the FortiClient endpoint that is registered to the selected FortiGate device. It also displays an icon that represents the operating system on the FortiClient endpoint. You can hover over each device to view device details.
User	Displays the name of the user logged into the FortiClient endpoint.
IP address	Displays the IP address of the FortiClient endpoint.
Status	Displays one of the following statuses for the FortiClient endpoint: <ul style="list-style-type: none"> • Online • Offline • Registered-Online • Registered-Offline • Un-Registered

FortiClient Version	Displays the version of FortiClient software installed on the FortiClient endpoint.
FortiClient Profile	Displays the name of the FortiClient profile that is assigned to the FortiClient endpoint.
Compliance	<p>Displays one of the following icons of compliance statuses for the FortiClient endpoint:</p> <ul style="list-style-type: none"> • Compliant • Endpoint is not compliant with FortiClient profile • Quarantined • FortiTelemetry is disabled • Exempt <p>Hover the mouse over the compliance status icon to view more information. Additional information about why the endpoint is not compliant may also be displayed.</p>

Monitoring FortiClient endpoints by compliance status

To monitor FortiClient endpoints by compliance status:

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.
3. Click *By Compliance Status*.
The list of FortiClient endpoints is displayed by compliance status.
4. In the *Device* column, click the compliance status to hide and display its list of FortiClient endpoints.
For example, click *Noncompliant* to hide and display the list of FortiClient endpoints with a status of noncompliant.
5. In the *Compliance* column, hover the mouse over the compliance status to view more details.

Monitoring FortiClient endpoints by interface

To monitor FortiClient endpoints by interface:

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.
3. Click *By Interface*.
The list of FortiClient endpoints is displayed by compliance status.
4. In the *Device* column, click *Undetected* or the name of the interface to hide and display its list of FortiClient endpoints.

Exempting non-compliant FortiClient endpoints

You can exempt FortiClient endpoints that are non-compliant from the compliance rules to allow the endpoints to access the network.

To exempt non-compliant FortiClient endpoints:

1. Go to *FortiClient Manager > Monitor*.
2. In the tree menu, select a FortiGate device.
3. Select one or more FortiClient endpoints.
4. Right-click the selected FortiClient endpoint, and select *Exempt this device* or *Exempt all devices of this type*.
The FortiClient endpoint is exempt from the compliance rules.
5. Install the configuration changes to the FortiGate device.

FortiClient profiles

The *FortiClient Manager > Profiles* pane allows you to create and manage FortiClient profile packages and profiles for endpoints. You can create profile packages of profiles for endpoints that are running the following operating systems: Windows, Mac, iOS, and Android.

The following information is displayed on the *FortiClient Manager > FortiClient Profiles* pane:

Profile Package	In the <i>Profile Package</i> menu, you can select to create, rename, or delete a FortiClient profile package.
Assign Profile Package	Assigns the selected FortiClient profile package to a device.
Install Wizard	Click to launch the Install Wizard to install device settings to devices. This process installs the FortiClient profile package that is assigned to the device.

Viewing profile packages

To view profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Click *All Profile Packages*.

The following options are available in the toolbar:

Create New	Click to create a new FortiClient profile package.
Rename	Click to rename the selected profile package.
Delete	Click to delete the selected profile package and all of its profiles.

The following information is displayed in the content pane:

Package Name	Displays the name of the profile package.
Device Targets	Displays the name of the device to which the profile package has been assigned.

Viewing FortiClient profiles

To view FortiClient profiles:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. In the *All Profile Packages* tree menu, click a profile.

The following options are available in the toolbar:

Create New	Click to create a new FortiClient profile for the selected FortiClient profile package.
Edit	Select a profile, and click <i>Edit</i> to edit the profile. Alternatively, double click the profile to open the <i>Edit FortiClient Profile</i> pane.
Delete	Select a profile, and click <i>Delete</i> to delete the profile from the selected FortiClient profile package. Alternately, right-click a profile, and select <i>Delete</i> .
Import	Select to import a FortiClient profile from an existing device or VDOM into the selected FortiClient profile package.
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns.

The following information is displayed in the content pane:

Seq.#	Displays the sequence number of the FortiClient profile.
FortiClient Profile	Displays the name of the FortiClient profile for the selected FortiClient profile package.
Assign To	Displays the device groups, user groups, and users associated with the FortiClient profile.
Comments	Displays any comments about the FortiClient profile.
Non-Compliance Action	Displays the selected non-compliance action settings from the FortiClient profile. The settings include: <i>Warning</i> , <i>Block</i> , or <i>Auto-Update</i> .

Creating FortiClient profile packages

FortiClient profile packages contain one or more FortiClient profiles. You assign FortiClient profile packages to devices or VDOMs.

FortiManager includes a default FortiClient profile package, and you can create multiple profiles for the profile package.

You can also create custom FortiClient profile packages and profiles.

To create profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. From the *Profile Package* menu, select *Create New*.
3. Type a name, and click *OK*.

Creating FortiClient profiles

You can create one or more FortiClient profiles in a FortiClient profile package. The FortiClient profile identifies the FortiGate compliance rules and the non-compliance action to apply to endpoints that fail to meet the compliance rules.



The FortiClient profile does not contain any configuration information for FortiClient. The FortiClient profile only identifies the compliance rules that FortiClient endpoints must meet to maintain access to the network.

You can enable compliance rules for the following categories in a FortiClient profile:

- Endpoint Vulnerability Scan on Client
- System Compliance
- Security Posture Check

For each category, you can specify how to handle endpoints that fail to meet the compliance rules. You can choose to block non-compliant endpoints from network access, or you can warn non-compliant endpoints, but allow network access. For example, you could set the non-compliance action to *Block* for *Endpoint Vulnerability Scan on Client*, and you can set the non-compliance action to *Warning* for *Security Posture Check*.

For more information on configuring FortiClient Profiles and Endpoint Control, see the *FortiOS Handbook* and the *FortiClient Administration Guide*.

FortiClient profiles can be created, edited, deleted, and imported from devices using the right-click menu and toolbar selections.



In FortiOS, this feature is found at *Security Profiles > FortiClient Profiles*.

To create a new FortiClient profile:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. In the tree menu, select the FortiClient profile package in which to create profiles.
3. In the content pane, click *Create New*.

The *Create New FortiClient Profile* pane opens.

Create New FortiClient Profile	
Profile Name	<input type="text"/>
Comments	<input type="text"/>
Assign Profile To	
Device Groups	<input type="text" value="Click to add ..."/>
User Groups	<input type="text" value="Click to add ..."/>
Users	<input type="text" value="Click to add ..."/>
Address	<input type="text" value="Click to add ..."/>
On-Net Detection By Address	<input type="text" value="Click to add ..."/>

4. Enter the following information:

Profile Name	Type a name for the new FortiClient profile. When creating a new FortiClient profile, XSS vulnerability characters are not allowed.
Comments	(Optional) Type a profile description.
Assign Profile To	Identify where to assign the profile: <ul style="list-style-type: none"> • Device Groups: Select device groups in the dropdown list. • User Groups: Select user groups in the dropdown list. • Users: Select users in the dropdown list. • Address: Select addresses in the dropdown list. You can assign the profile to user groups and users when using Active Directory authentication or RADIUS authentication for VPN.
On-Net Detection By Address	Identify whether to use an address to detect when endpoints are on-net. Select the address(es) from the list.

5. Set the compliance rules and non-compliance action for *Endpoint Vulnerability Scan on Client*:

Endpoint Vulnerability Scan on Client	Toggle <i>ON</i> to add a rule about <i>Vulnerability Scanning on Client</i> . When toggled <i>ON</i> , the Vulnerability Scanning module must be enabled in FortiClient on endpoints. Toggle <i>OFF</i> to exclude <i>Vulnerability Scanning on Client</i> from the compliance rules.
Non-compliance action	Specify how to handle endpoints that fail to meet the compliance rules for <i>Endpoint Vulnerability Scan on Client</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.
Vulnerability quarantine level	When <i>Endpoint Vulnerability Scan on Client</i> is toggled to <i>ON</i> , you can select a minimum quarantine level from the <i>Vulnerability quarantine level</i> list. Endpoints with detected vulnerabilities that hit the minimum severity level or higher are quarantined.

6. Set the compliance rules and non-compliance action for *System Compliance*:

System compliance	Toggle <i>ON</i> to enable compliance rules for <i>System compliance</i> and display options for rules. Toggle <i>OFF</i> to exclude system compliance from the compliance rules.
Minimum FortiClient Version	Toggle <i>ON</i> to add a rule about minimum FortiClient version. When toggled <i>ON</i> , endpoints must have the minimum version or higher of FortiClient installed to remain compliant. Specify the minimum version in the <i>Windows endpoints</i> and <i>Mac endpoints</i> boxes. Toggle <i>OFF</i> to remove a rule about minimum FortiClient version from the compliance rules.

Windows endpoints	When <i>Minimum FortiClient Version</i> is toggled <i>ON</i> , you can type the minimum version of FortiClient that is required on endpoints running a Windows operating system.
Mac endpoints	When <i>Minimum FortiClient Version</i> is toggled <i>ON</i> , you can type the minimum version of FortiClient that is required on endpoints running a Macintosh operating system.
Upload logs to FortiAnalyzer	<p>Toggle <i>ON</i> to add a rule about logging. When toggled <i>ON</i>, FortiClient must send logs to FortiAnalyzer for the endpoint to remain compliant. Select which of the following FortiClient logs must be sent to FortiAnalyzer:</p> <ul style="list-style-type: none"> • Traffic • Vulnerability • Event <p>Toggle <i>OFF</i> to remove a rule about logging from the compliance rules.</p>
Non-compliance action	Specify how to handle endpoints that fail to meet the compliance rules for <i>System Compliance</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.

7. Set the compliance rules and non-compliance action for *Security Posture Check*:

Security Posture Check	<p>Toggle <i>ON</i> to enable compliance rules for <i>Security Posture Check</i> and display more options. When toggled <i>ON</i>, select which modules must be enabled in FortiClient for endpoints to remain compliant.</p> <p>Toggle <i>OFF</i> to remove rules about <i>Security Posture Check</i> from the compliance rules.</p>
Real-time Protection	<p>Toggle <i>ON</i> to add a rule about real-time protection to the compliance rules. When toggled <i>ON</i>, FortiClient must have real-time protection enabled for endpoints to remain compliant.</p> <p>Toggle <i>OFF</i> to remove a rule about real-time protection from the compliance rules.</p>
Up-to-date signatures	<p>Toggle <i>ON</i> to add a rule about up-to-date signatures to the compliance rules. When toggled <i>ON</i>, FortiClient real-time protection must have up-to-date signatures for endpoints to remain compliant.</p> <p>Toggle <i>OFF</i> to remove a rule about up-to-date signatures from the compliance rules.</p>
Scan with FortiSandbox	<p>Toggle <i>ON</i> to add a rule about FortiSandbox scanning to the compliance rules. When toggled <i>ON</i>, FortiClient real-time protection must have FortiSandbox scanning enabled for endpoints to remain compliant.</p> <p>Note: A FortiSandbox device is required, and the device must be configured to work with FortiClient.</p> <p>Toggle <i>OFF</i> to remove a rule about FortiSandbox scanning from the compliance rules.</p>

	Non-compliance action	Specify how to handle endpoints that fail to meet the compliance rules about <i>Real-time Protection</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.
Third party AntiVirus on Windows		<p>Toggle <i>ON</i> to add a rule about third-party antivirus software for endpoints running a Windows operating system to the compliance rules. When toggled <i>ON</i>, endpoints running a Windows operating system must have recognized third-party antivirus software installed for endpoints to remain compliant.</p> <p>Note: <i>Real-time Protection</i> must be toggled <i>OFF</i> before you can toggle on <i>Third party AntiVirus on Windows</i>.</p> <p>Toggle <i>OFF</i> to remove the rule about third-party antivirus software from the compliance rules.</p>
Web Filter		<p>Toggle <i>ON</i> to add a rule about <i>Web Filter</i> to the compliance rules and display more options.</p> <p>Toggle <i>OFF</i> to exclude a rule about <i>Web Filter</i> from the compliance rules.</p>
	Profile	When <i>Web Filter</i> is toggled <i>ON</i> , you can select a web filter profile. A default profile is selected by default.
Application Firewall		<p>Toggle <i>ON</i> to add a rule about <i>Application Firewall</i> to the compliance rules and display more options.</p> <p>Toggle <i>OFF</i> to exclude the setting from the compliance rules.</p>
	Application Control Sensor	When <i>Application Firewall</i> is toggled <i>ON</i> , you can select an application control sensor. A default application control sensor is selected by default.
	Non-compliance action	Specify how to handle endpoints that fail to meet the compliance rules for <i>Security Posture Check</i> . Select <i>Block</i> to block not-compliant endpoints from network access. Select <i>Warning</i> to warn not-compliant endpoints, but allow network access.

8. Click *OK*.

Editing FortiClient profiles

To edit a FortiClient profile:

1. Right-click a profile, and select *Edit*. The *Edit FortiClient Profile <name>* pane is displayed.
2. Edit the settings, and click *OK*.

Deleting FortiClient profiles

To delete a FortiClient profile:

1. Right-click a profile, and select *Delete*.
2. Click *OK* in the confirmation dialog box to delete the profile.

Importing FortiClient profiles

You can import FortiClient profiles from FortiGate.

To import a FortiClient profile:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Select a profile package, and click *Import*. The *Import* dialog box is displayed.
3. Enter the following information:

Import From Device	Select a device from which to import the profile or profiles from the dropdown list. This list will include all the devices available in the ADOM.
Profile	Select the profile to import.
New Name	Select to create a new name for the profile being imported, and then type the name in the field.

4. Click *OK*. The profile is imported into the selected profile package.

Assigning profile packages

To assign profile packages:

1. Go to *FortiClient Manager > FortiClient Profiles*.
2. Select a profile package, and click *Assign Profile Package*. The *Assign Profile Package* dialog box is displayed.
3. Select one or more devices, and click *OK*. The profile package is assigned to the device(s).
4. Install the configuration changes to the FortiGate device. See [Configuring a device on page 125](#) for more information.

FortiGuard

The FortiGuard Distribution Network (FDN) provides FortiGuard services for your FortiManager system and its managed devices and FortiClient agents. The FDN is a world-wide network of FortiGuard Distribution Servers (FDS), which update the FortiGuard services on your FortiManager system on a regular basis so that your FortiManager system is protected against the latest threats.

The FortiGuard services available on the FortiManager system include:

- Antivirus and IPS engines and signatures
- Web filtering and email filtering rating databases and lookups (select systems)
- Vulnerability scan and management support for FortiAnalyzer

To view and configure these services, go to *FortiGuard > Settings*.

In FortiGuard Management, you can configure the FortiManager system to act as a local FDS, or use a web proxy server to connect to the FDN. FortiManager systems acting as a local FDS synchronize their FortiGuard service update packages with the FDN, then provide FortiGuard these updates and look up replies to your private network's FortiGate devices. The local FDS provides a faster connection, reducing Internet connection load and the time required to apply frequent updates, such as antivirus signatures, to many devices.

As an example, you might enable FortiGuard services to FortiGate devices on the built-in FDS, then specify the FortiManager system's IP address as the override server on your devices. Instead of burdening your Internet connection with all the devices downloading antivirus updates separately, the FortiManager system would use the Internet connection once to download the FortiGate antivirus package update, then redistribute the package to the devices.

FortiGuard Management also includes firmware revision management. To view and configure firmware options, go to *FortiGuard > Firmware Images*. You can download these images from the Customer Service & Support portal to install on your managed devices or on the FortiManager system.

Before you can use your FortiManager system as a local FDS, you must:

- Register your devices with Fortinet Customer Service & Support and enable the FortiGuard service licenses. See your device documentation for more information on registering your products.
- If the FortiManager system's Unregistered Device Options do not allow service to unregistered devices, add your devices to the device list, or change the option to allow service to unregistered devices. For more information, see the *FortiManager CLI Reference*.

For information about FDN service connection attempt handling or adding devices, see [Device Manager on page 106](#).

- Enable and configure the FortiManager system's built-in FDS. For more information, see [Configuring network interfaces on page 43](#).
- Connect the FortiManager system to the FDN.

The FortiManager system must retrieve service update packages from the FDN before it can redistribute them to devices and FortiClient agents on the device list. For more information, see [Connecting the built-in FDS to the FDN on page 357](#).

- Configure each device or FortiClient endpoint to use the FortiManager system's built-in FDS as their override server. You can do this when adding a FortiGate system. For more information, see [Adding devices on page 107](#).

This section contains the following topics:

- [Settings](#)
- [Configuring devices to use the built-in FDS](#)
- [Configuring FortiGuard services](#)
- [Logging events related to FortiGuard services](#)
- [Restoring the URL or antispam database](#)
- [Licensing status](#)
- [Package management](#)
- [Query server management](#)
- [Firmware images](#)



For information on current security threats, virus and spam sample submission, and FortiGuard service updates available through the FDN, including antivirus, IPS, web filtering, and email filtering, see the FortiGuard Center website, <https://fortiguard.com/>.

Settings

FortiGuard > Settings provides a central location for configuring and enabling your FortiManager system's built-in FDS as an FDN override server.

By default, this option is enabled. After configuring FortiGuard and configuring your devices to use the FortiManager system as their FortiGuard server, you can view overall and per device statistics on FortiGuard service benefits.

To operate in a closed network, disable communication with the FortiGuard server. See [Operating as an FDS in a closed network on page 358](#).

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server ☒

Communication with FortiGuard Server ☒ Global Servers ☐ Servers Located in US Only

Enable Antivirus and IPS Service ☐

Enable Web Filter Service ☐

Enable Email Filter Service ☐

Server Override Mode ☐ Strict (Access Override Server Only) ☒ Loose (Allow Access Other Servers)

FortiGuard Antivirus and IPS Settings >

FortiGuard Web Filter and Email Filter Settings >

Override FortiGuard Server (Local FortiManager) >

Apply

Enable communication with FortiGuard servers.

When toggled *OFF*, you must manually upload packages, databases, and licenses to your FortiManager. See [Operating as an FDS in a closed network on page 358](#).

FortiManager Administration Guide

Fortinet Technologies Inc.

Communication with FortiGuard Server	Select <i>Servers Located in the US Only</i> to limit communication to FortiGuard servers located in the USA. Select <i>Global Servers</i> to communicate with servers anywhere.
Enable Antivirus and IPS Service	Toggle <i>ON</i> to enable antivirus and intrusion protection service. When on, select what versions <i>FortiGate</i> , <i>FortiClient</i> , <i>FortiAnalyzer</i> , and <i>FortiMail</i> to download updates for.
Enable Web Filter and Services	Toggle <i>ON</i> to enable web filter services. When uploaded to FortiManager, the Web Filter database is displayed.
Enable Email Filter Services	Toggle <i>ON</i> to enable email filter services. When uploaded to FortiManager, the Email Filter database is displayed.
Server Override Mode	Select <i>Strict (Access Override Server Only)</i> or <i>Loose (Allow Access Other Servers)</i> override mode.
FortiGuard Antivirus and IPS Settings	Configure antivirus and IPS settings. See FortiGuard antivirus and IPS settings on page 355 .
FortiGuard Web Filter and Email Filter Settings	Configure web and email filter settings. See FortiGuard web and email filter settings on page 356 .
Override FortiGuard Server (Local FortiManager)	Configure web and email filter settings. See Override FortiGuard server (Local FortiManager) on page 357 .

FortiGuard antivirus and IPS settings

In this section you can enable settings for FortiGuard Antivirus and IPS settings. The following settings are available:

Use Override Server Address for FortiGate/FortiMail	Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries. To override the default server for updating FortiGate/FortiMail device's FortiGuard services, see Overriding default IP addresses and ports on page 364 .
Allow Push Update	Configure to allow urgent or critical updates to be pushed directly to the FortiManager system when they become available on the FDN. The FortiManager system immediately downloads these updates. To enable push updates, see Enabling push updates on page 362 .
Use Web Proxy	Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy. To enable updates using a web proxy, see Enabling updates through a web proxy on page 364 .
Scheduled Regular Updates	Configure when packages are updated without manually initiating an update request. To schedule regular service updates, see Scheduling updates on page 365 .

Advanced

Enables logging of service updates and entries.

If either option is not turned on, you will not be able to view these entries and events when you select *View FDS and FortiGuard Download History*.

FortiGuard web and email filter settings

In this section you can enable settings for FortiGuard Web Filter and Email Filter.

FortiGuard Web Filter and Email Filter Settings ▾

Connection to FDS Server(s)

☐ OFF

Use Override Server Address for FortiClient

☐ OFF

Use Override Server Address for FortiGate/FortiMail

☐ OFF

Use Web Proxy

Polling Frequency

Poll Every

0

Hour

10

Minute

Log Settings

☒ ON

Log FortiGuard Server Update Events

FortiGuard Web Filtering

☐ Log URL disabled ☒ Log non-url events ☐ Log all URL lookups

FortiGuard Anti-spam

☐ Log Spam disabled ☒ Log non-spam events ☐ Log all Spam lookups

FortiGuard Anti-virus Query

☐ Log Virus disabled ☒ Log non-virus events ☐ Log all Virus lookups

Override FortiGuard Server (Local FortiManager) >

The following settings are available:

Connection to FDS Server(s)

Configure connections for overriding the default built-in FDS or web proxy server for web filter and email filter settings.

To override an FDS server for web filter and email filter services, see [Overriding default IP addresses and ports on page 364](#).

To enable web filter and email filter service updates using a web proxy server, see [Enabling updates through a web proxy on page 364](#).

Use Override Server Address for FortiClient

Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.

Use Override Server Address for FortiGate/FortiMail

Configure to override the default built-in FDS so that you can use a port or specific FDN server. Select the add icon to add additional override servers, up to a maximum of ten. Select the delete icon to remove entries.

To override the default server for updating FortiGate device's FortiGuard services, see [Overriding default IP addresses and ports on page 364](#).

Use Web Proxy

Configure the FortiManager system's built-in FDS to connect to the FDN through a web proxy. IPv4 and IPv6 are supported.

To enable updates using a web proxy, see [Enabling updates through a web proxy on page 364](#).

Polling Frequency

Configure how often polling is done.

Log Settings

Configure logging of FortiGuard web filtering, email filter, and antivirus query events.

- *Log FortiGuard Server Update Events*: enable or disable
- *FortiGuard Web Filtering*: Choose from *Log URL disabled*, *Log non-URL events*, and *Log all URL lookups*.
- *FortiGuard Anti-spam*: Choose from *Log Spam disabled*, *Log non-spam events*, and *Log all Spam lookups*.
- *FortiGuard Anti-virus Query*: Choose from *Log Virus disabled*, *Log non-virus events*, and *Log all Virus lookups*.

To configure logging of FortiGuard web filtering and email filtering events, see [Logging FortiGuard web or email filter events on page 367](#).

Override FortiGuard server (Local FortiManager)

Configure and enable alternate FortiManager FDS devices, rather than using the local FortiManager system. You can set up as many alternate FDS locations, and select what services are used. The following settings are available:

Additional number of Private FortiGuard Servers (Excluding This One)

Select the add icon to add a private FortiGuard server. Select the delete icon to remove entries.

When adding a private server, you must type its IP address and time zone.

Enable Antivirus and IPS Update Service for Private Server

When one or more private FortiGuard servers are configured, update antivirus and IPS through this private server instead of using the default FDN.

This option is available only when a private server has been configured.

Enable Web Filter and Email Filter Update Service for Private Server

When one or more private FortiGuard servers are configured, update the web filter and email filter through this private server instead of using the default FDN.

This option is available only when a private server has been configured.

Allow FortiGates to Access Public FortiGuard Servers When Private Servers Unavailable

When one or more private FortiGuard servers are configured, managed FortiGate units will go to those private servers for FortiGuard updates. Enable this feature to allow those FortiGate units to then try to access the public FDN servers if the private servers are unreachable.

This option is available only when a private server has been configured.



The FortiManager system's network interface settings can restrict which network interfaces provide FDN services. For more information, see [Configuring network interfaces on page 43](#).

Connecting the built-in FDS to the FDN

When you enable the built-in FDS and initiate an update either manually or by a schedule, the FortiManager system attempts to connect to the FDN.

If all connection attempts to the server list fail, the connection status will be *Disconnected*.

If the connection status remains *Disconnected*, you may need to configure the FortiManager system's connection to the FDN by:

- overriding the default IP address and/or port
- configuring a connection through a web proxy

After establishing a connection with the FDN, the built-in FDS can receive FortiGuard service update packages, such as antivirus engines and signatures or web filtering database updates, from the FDN.

To enable the built-in FDS:

1. Go to *FortiGuard > Settings*.
2. Enable the types of FDN services that you want to provide through your FortiManager system's built-in FDS. For more information, see [Configuring FortiGuard services on page 362](#).
3. Click *Apply*.

The built-in FDS attempts to connect to the FDN.



If the built-in FDS is unable to connect, you may need to enable the selected services on a network interface. For more information, see [Configuring network interfaces on page 43](#).

If you still cannot connect to the FDN, check routes, DNS, and any intermediary firewalls or NAT devices for policies that block necessary FDN ports and protocols. For additional FDN troubleshooting information, including FDN server selection, see [FDN port numbers and protocols on page 365](#).

See the *FortiOS HandBook: FortiGuard Licensing for FortiGates with Limited or No Connectivity* document in the Fortinet Document Library at <https://docs.fortinet.com/fortigate/admin-guides> for more information.

Operating as an FDS in a closed network

The FortiManager can be operated as a local FDS server when it is in a closed network with no internet connectivity.

Without a connection to a FortiGuard server, update packages and licenses must be manually downloaded from support, and then uploaded to the FortiManager.



As databases can be large, we recommend uploading them using the CLI. See [Uploading packages with the CLI](#).

Go to *FortiGuard > Settings* to configure FortiManager as a local FDS server and to upload update packages and license.

FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server

Enable Antivirus and IPS Service

FortiGate	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	<input type="checkbox"/> 5.6
FortiClient	<input type="checkbox"/> All v4	<input type="checkbox"/> 5.0	<input type="checkbox"/> 5.2	<input type="checkbox"/> 5.4	
FortiAnalyzer	<input type="checkbox"/> All v4	<input checked="" type="checkbox"/> 5.0	<input checked="" type="checkbox"/> 5.2	<input checked="" type="checkbox"/> 5.4	
FortiMail	<input type="checkbox"/> All v4	<input type="checkbox"/> All v5			

Enable Web Filter Service

Enable Email Filter Service

Upload Options for FortiGate/FortiMail

Antivirus/IPS Packages	<input type="button" value="Upload"/>
Web Filter Database	<input type="button" value="Upload"/>
Email Filter Database	<input type="button" value="Upload"/>
Service License	<input type="button" value="Upload"/>

Upload Options for FortiClient

Antivirus/IPS Packages	<input type="button" value="Upload"/>
------------------------	---------------------------------------

Enable Communication with FortiGuard Servers

Toggle *OFF* to disable communication with the FortiGuard servers.

Enable Antivirus and IPS Service

Toggle *ON* to enable antivirus and intrusion protection service. When on, select what versions *FortiGate*, *FortiClient*, *FortiAnalyzer*, and *FortiMail* to download updates for.

Enable Web Filter Services

Toggle *ON* to enable web filter services. When uploaded to FortiManager, the Web Filter database is displayed.

Enable Email Filter Services

Toggle *ON* to enable email filter services. When uploaded to FortiManager, the Email Filter database is displayed.

Upload Options for FortiGate/FortiMail

AntiVirus/IPS Packages

Select to upload antivirus and IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box. Click *OK* to upload the package to FortiManager.

Web Filter Database

Select to upload the web filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box. Click *OK* to upload the package to FortiManager. As the database can be large, uploading with the CLI is recommended. See the instructions below.

Email Filter Database

Select to upload the email filter database. Browse for the file you downloaded from the Customer Service & Support portal on your management computer. Click **OK** to upload the package to FortiManager.

As the database can be large, uploading with the CLI is recommended. See the instructions below.

Service License

Select to import the FortiGate license. Browse for the file on your management computer, or drag and drop the file onto the dialog box. Click **OK** to upload the package to FortiManager.

A license file can be obtained from support by requesting your account entitlement for the device.

Upload Options for FortiClient**AntiVirus/IPS Packages**

Select to upload the FortiClient AntiVirus/IPS packages. Browse for the file you downloaded from the Customer Service & Support portal on your management computer, or drag and drop the file onto the dialog box. Click **OK** to upload the package to FortiManager.

Uploading packages with the CLI

Packages and licenses can be uploaded using the CLI. This should be used when the packages being uploaded are large, like database packages.

To upload packages and license files using the CLI:

1. If not already done, disable communications with the FortiGuard server and enable a closed network with the following CLI commands:


```
config fmupdate publicnetwork
  set status disable
end
```
2. Upload an update package or license:
 - a. Load the package or license file to an FTP, SCP, or TFTP server
 - b. Run the following CLI command:


```
execute fmupdate { ftp | scp | tftp } import < av-ips | fct-av | url | spam |
file-query | license-fgt | license-fct | custom-url | dcomp > <remote_
file> <ip> <port> <remote_path> <user> <password>
```

Configuring devices to use the built-in FDS

After enabling and configuring the FortiManager system's built-in FDS, you can configure devices to use the built-in FDS by providing the FortiManager system's IP address and configured port as their override server.

Devices are not required to be registered with FortiManager system's *Device Manager* to use the built-in FDS for FortiGuard updates and services.

Procedures for configuring devices to use the built-in FDS vary by device type. See the documentation for your device for more information.



If you are connecting a device to a FortiManager system's built-in FDS, some types of updates, such as antivirus engine updates, require you to enable SSH and HTTPS Administrative Access on the network interface which will receive push updates. See [Network on page 43](#) for details.

Matching port settings

When configuring a device to override default FDN ports and IP addresses with that of a FortiManager system, the default port settings for the device's update or query requests may not match the listening port of the FortiManager system's built-in FDS. If this is the case, the device's requests will fail. To successfully connect them, you must match the devices' port settings with the FortiManager system's built-in FDS listening ports.

For example, the default port for FortiGuard antivirus and IPS update requests is TCP 443 on FortiOS v4.0 and higher, but the FortiManager system's built-in FDS listens for those requests on TCP 8890. In this case, the FortiGate unit's update requests would fail until you configure the unit to send requests on TCP 8890.

In some cases, the device may not be configurable; instead, you must configure the FortiManager system to listen on an alternate port.

Handling connection attempts from unregistered devices

The built-in FDS replies to FortiGuard update and query connections from devices registered with the device manager's device list. If the FortiManager is configured to allow connections from unregistered devices, unregistered devices can also connect.

For example, you might choose to manage a FortiGate unit's firmware and configuration locally (from its GUI), but use the FortiManager system when the FortiGate unit requests FortiGuard antivirus and IPS updates. In this case, the FortiManager system considers the FortiGate unit to be an unregistered device, and must decide how to handle the connection attempt. The FortiManager system will handle the connection attempt based on how it is configured. Connection attempt handling is only configurable via the CLI.

To configure connection attempt handling:

1. Go to the *CLI Console* widget in the *System Settings > Dashboard* pane. For information on widget settings, see [Customizing the dashboard on page 475](#).
2. Click inside the console to connect.
3. To configure the system to add unregistered devices and allow service requests, type the following CLI command lines:

```
config system admin setting
    set unreg_dev_opt add_allow_service
end
```
4. To configure the system to add unregistered devices but deny service requests, type the following CLI command lines:

```
config system admin setting
    set unreg_dev_opt add_no_service
end
```

For more information, see the *FortiManager CLI Reference*.

Configure a FortiManager without Internet connectivity to access a local FortiManager as FDS

By default, FortiManager connects to the public FDN to download security feature updates, including databases and engines for security feature updates such as Antivirus and IPS. Your FortiManager can be configured to use a second, local FortiManager for FDS updates.

To use a second FortiManager as the FDS:

1. Go to *FortiGuard > Settings*.
2. Ensure that *Communication with FortiGuard Server* is set to *Global Servers*.
3. Under *FortiGuard Antivirus and IPS Settings*:
 - a. Turn on *Use Override Server Address for FortiGate/FortiMail* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8890.
4. Under *FortiGuard Web Filter and Email Filter Settings*:
 - a. Turn on *Use Override Server Address for FortiGate/FortiMail* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8900.
 - b. If required, turn on *Use Override Server Address for FortiClient* and enter the IP address of the FortiManager unit being used as the FDS, and port number 8901.
5. Click *Apply*.

The FortiManager will use the second FortiManager unit as the FDS.

Configuring FortiGuard services

FortiGuard Management provides a central location for configuring how the FortiManager system accesses the FDN and FDS, including push updates. The following procedures explain how to configure FortiGuard services and configuring override and web proxy servers, if applicable.

If you need to host a custom URL list that are rated by the FortiGate unit, you can import a list using the CLI.

- [Enabling push updates](#)
- [Enabling updates through a web proxy](#)
- [Overriding default IP addresses and ports](#)
- [Scheduling updates](#)
- [Accessing public FortiGuard web and email filter servers](#)

Enabling push updates

When an urgent or critical FortiGuard antivirus or IPS signature update becomes available, the FDN can push update notifications to the FortiManager system's built-in FDS. The FortiManager system then immediately downloads the update.

To use push update, you must enable both the built-in FDS and push updates. Push update notifications will be ignored if the FortiManager system is not configured to receive them. If TCP port 443 downloads must occur through a web proxy, you must also configure the web proxy connection. See [Enabling updates through a web proxy on page 364](#).

If push updates must occur through a firewall or NAT device, you may also need to override the default push IP address and port.

For example, overriding the push IP address can be useful when the FortiManager system has a private IP address, and push connections to a FortiManager system must traverse NAT. Normally, when push updates are enabled, the FortiManager system sends its IP address to the FDN; this IP address is used by the FDN as the destination for push messages; however, if the FortiManager system is on a private network, this IP address may be a private IP address, which is not routable from the FDN – causing push updates to fail.

To enable push through NAT, type a push IP address override, replacing the default IP address with an IP address of your choice such as the NAT device's external or virtual IP address. This causes the FDN to send push packets to the override IP address, rather than the FortiManager system's private IP address. The NAT device can then forward the connection to the FortiManager system's private IP address.



The built-in FDS may not receive push updates if the external IP address of any intermediary NAT device is dynamic (such as an IP address from PPPoE or DHCP). When the NAT device's external IP address changes, the FortiManager system's push IP address configuration becomes out-of-date.

To enable push updates to the FortiManager system:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see [FortiGuard antivirus and IPS settings on page 355](#).
3. Toggle **ON** beside *Allow Push Update*.
4. If there is a NAT device or firewall between the FortiManager system and the FDN which denies push packets to the FortiManager system's IP address on UDP port 9443, type the IP Address and/or Port number on the NAT device which will forward push packets to the FortiManager system. The FortiManager system will notify the FDN to send push updates to this IP address and port number.
 - *IP Address* is the external or virtual IP address on the NAT device for which you will configure a static NAT or port forwarding.
 - *Port* is the external port on the NAT device for which you will configure port forwarding.
5. Click *Apply*.
6. If you performed step 4, also configure the device to direct that IP address and/or port to the FortiManager system.
 - If you entered a virtual IP address, configure the virtual IP address and port forwarding, and use static NAT mapping.
 - If you entered a port number, configure port forwarding; the destination port must be UDP port 9443, the FortiManager system's listening port for updates.

To enable push through NAT in the CLI:

Enter the following commands:

```
config fmupdate fds-setting
config push-override-to-client
set status enable
config announce-ip
edit 1
set ip <override IP that FortiGate uses to download updates from FortiManager>
set port <port that FortiManager uses to send the update announcement>
```

```
        end
    end
end
```

Enabling updates through a web proxy

If the FortiManager system's built-in FDS must connect to the FDN through a web (HTTP or HTTPS) proxy, you can specify the IP address and port of the proxy server.

If the proxy requires authentication, you can also specify a user name and password.

To enable updates to the FortiManager system through a proxy:

1. Go to *FortiGuard > Settings*.
2. If configuring a web proxy server to enable web and email filtering updates, expand *FortiGuard Web Filter and Email Filter Settings*.
3. If configuring a web proxy to enable antivirus and IPS updates, expand *FortiGuard Antivirus and IPS Settings*.
4. Toggle *ON* beside *Use Web Proxy* and enter the IP address and port number of the proxy.
5. If the proxy requires authentication, enter the user name and password.
6. Click *Apply*.

If the FDN connection status is *Disconnected*, the FortiManager system is unable to connect through the web proxy.

Overriding default IP addresses and ports

The FortiManager device's built-in FDS connects to the FDN servers using default IP addresses and ports. You can override these defaults if you want to use a port or specific FDN server that is different from the default.

To override default IP addresses and ports:

1. Go to *FortiGuard > Settings*.
2. If you want to override the default IP address or port for synchronizing with available FortiGuard antivirus and IPS updates, click the arrow to expand *FortiGuard Antivirus and IPS Settings*, then toggle *ON* beside *Use Override Server Address for FortiGate/FortiMail* and enter the IP address and/or port number for all FortiGate units.
3. If you want to override the FortiManager system's default IP address or port for synchronizing with available FortiGuard web and email filtering updates, click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
4. Toggle *ON* beside *Use Override Server Address for FortiGate/FortiMail* and/or *Use Override Server Address for FortiClient* and type the IP address and/or port number.
5. Click *Apply*.

If the FDN connection status remains disconnected, the FortiManager system is unable to connect with the configured override.

FDN port numbers and protocols

Both the built-in FDS and devices use certain protocols and ports to successfully request and receive updates from the FDN or override server. Any intermediary proxies or firewalls must allow these protocols and ports, or the connection will fail.

After connecting to the FDS, you can verify connection status on the FortiGuard Management page. For more information about connection status, see [Connecting the built-in FDS to the FDN on page 357](#).

Scheduling updates

Keeping the built-in FDS up-to-date is important to provide current FortiGuard update packages and rating lookups to requesting devices. This is especially true as new viruses, malware, and spam sources pop up on a very frequent basis. By configuring a scheduled update, you are guaranteed to have a relatively recent version of database updates.

A FortiManager system acting as an FDS synchronizes its local copies of FortiGuard update packages with the FDN when:

- you manually initiate an update request by selecting *Update Now*
- it is scheduled to poll or update its local copies of update packages
- if push updates are enabled, it receives an update notification from the FDN

If the network is interrupted when the FortiManager system is downloading a large file, it downloads all files again when the network resumes.

To schedule antivirus and IPS updates:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see [FortiGuard antivirus and IPS settings on page 355](#).
3. Toggle *ON* beside *Schedule Regular Updates*.
4. Specify an hourly, daily, or weekly schedule.
5. Click *Apply*.

To schedule Web Filtering and Email Filter polling:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Web Filter and Email Filter Settings*.
3. In *Polling Frequency*, select the number of hours and minutes of the polling interval.
4. Click *Apply*.



If you have formatted your FortiManager system's hard disk, polling and lookups will fail until you restore the URL and email filter databases. For more information, see [Restoring the URL or antispam database on page 368](#).

Accessing public FortiGuard web and email filter servers

You can configure the FortiManager system to allow the managed FortiGate units to access public FortiGuard web filter or email filter network servers in the event local FortiGuard web filter or email filter server URL lookups fail. You can specify private servers where the FortiGate units can send URL queries.

To access public FortiGuard web and email filter servers:

1. Go to *FortiGuard > Settings*.
2. Click the arrow beside *Override FortiGuard Server (Local FortiManager)*.
3. Click the add icon next to *Additional number of private FortiGuard servers (excluding this one)*. Select the delete icon to remove entries.
4. Type the *IP Address* for the server and select its *Time Zone*.
5. Repeat step 4 as often as required. You can include up to ten additional servers.
6. Select the additional options to set where the FDS updates come from, and if the managed FortiGate units can access these servers if the local FDS is not available.
 - Toggle *ON* beside *Enable Antivirus and IPS update Service for Private Server* if you want the FDS updates to come from a private server.
 - Toggle *ON* beside *Enable Web Filter and Email Filter Service for Private Server* if you want the updates to come from a private server.
 - Toggle *ON* beside *Allow FortiGates to Access Public FortiGuard Servers when Private Servers are Unavailable* if you want the updates to come from public servers in case the private servers are unavailable.
7. Click *Apply*.

Logging events related to FortiGuard services

You can log a variety of events related to FortiGuard services.



Logging events from the FortiManager system's built-in FDS requires that you also enable local event logging.

Logging FortiGuard antivirus and IPS updates

You can track FortiGuard antivirus and IPS updates to both the FortiManager system's built-in FDS and any registered FortiGate devices which use the FortiManager system's FDS.

To log updates and histories to the built-in FDS:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*; see [FortiGuard antivirus and IPS settings on page 355](#).

3. Under the *Advanced* heading, toggle *ON* beside *Log Update Entries from FDS Server*.
4. Click *Apply*.

To log updates to FortiGate devices:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Antivirus and IPS Settings*.
3. Under the *Advanced* heading, toggle *ON* beside *Log Update Histories for Each FortiGate*.
4. Click *Apply*.

Logging FortiGuard web or email filter events

You can track FortiGuard web filtering and email filtering lookup and non-events occurring on any registered FortiGate device which uses the FortiManager system's FDS.

Before you can view lookup and non-event records, you must enable logging for FortiGuard web filtering or email filter events.

To log rating queries:

1. Go to *FortiGuard > Settings*.
2. Click the arrow to expand *FortiGuard Web Filtering and Email Filter Settings*.
3. Configure the log settings, then click *Apply*:

Log FortiGuard Server Update Events	Enable or disable logging of FortiGuard server update events.
FortiGuard Web Filtering	
Log URL disabled	Disable URL logging.
Log non-URL events	Logs only non-URL events.
Log all URL lookups	Logs all URL lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-spam	
Log Spam disabled	Disable spam logging.
Log non-spam events	Logs email rated as non-spam.
Log all Spam lookups	Logs all spam lookups (queries) sent to the FortiManager system's built-in FDS by FortiGate devices.
FortiGuard Anti-virus Query	
Log Virus disabled	Disable virus logging.
Log non-virus events	Logs only non-virus events.
Log all Virus lookups	Logs all virus queries sent to the FortiManager system's built-in FDS by FortiGate devices.

Restoring the URL or antispam database

Formatting the hard disk or partition on FortiManager 3000 units and higher deletes the URL and antispam databases required to provide FortiGuard email filter and web filtering services through the built-in FDS. The databases will re-initialize when the built-in FDS is scheduled next, to synchronize them with the FDN.

Before formatting the hard disk or partition, you can back up the URL and antispam database using the CLI, which encrypts the file. You can also back up licenses as well. The databases can be restored by importing them using the CLI. If you have created a custom URL database, you can also backup or restore this customized database (for FortiGate units).

Licensing status

FortiManager includes a licensing overview page that allows you to view license information for all managed FortiGate devices. To view the licensing status, go to *FortiGuard > Licensing Status*.

This page displays the following information:

Refresh	Select the refresh icon to refresh the information displayed on this page.
Hide/Show license expired devices only	Toggle to hide and display devices with an expired license only.
Search	Use the search field to find a specific device in the table.
Device Name	The device name or host name. You can change the order that devices are listed by clicking the column title.
Serial Number	The device serial number
Platform	The device type, or platform.
ADOM	ADOM information. You can change the order that ADOMs are listed by clicking the column title.
Antivirus	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
IPS	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Email Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Web Filtering	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Mobile Malware	The license status and expiration date. You can change the order that devices are listed by clicking the column title.
Support	The license status and expiration date. You can change the order that devices are listed by clicking the column title.

Icon states:

- Green: License OK
- Orange: License will expire soon
- Red: License has expired

Package management

Antivirus and IPS signature packages are managed in *FortiGuard > Package Management*. Packages received from FortiGuard and the service status of managed devices are listed in *Receive Status* and *Service Status*, respectively.

Receive status

To view packages received from FortiGuard, go to *FortiGuard > Package Management > Receive Status*. This page lists received packages, grouped by platform.

The following information is displayed:

Refresh	Select to refresh the table.
Show Used Object Only	Clear to show all package information. Select to show only relevant package information.
Search	Use the search field to find a specific object in the table.
Object Name	The name of the object.
Object Type	The type of object for the package.
Package Received	The name of the package.
Latest Version (Release Date/Time)	The package version.
Size	The size of the package.
To Be Deployed Version	The package version that is to be deployed. Select <i>Change</i> to change the version.
Update History	Select the icon to view the package update history.

Deployed version

To change the to be deployed version of a received packaged, click *Change* in the *To Be Deployed Version* column for the package.

The *Change Version* dialog box is displayed, allowing you to select an available version from the dropdown list.

Update history

When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Service status

To view service statuses, go to *FortiGuard > Package Management > Service Status*. The service status information can be displayed by installed package name or by device name.

The following options are available in the toolbar:

Push Pending	Select the device or devices in the list, then click <i>Push Pending</i> in the toolbar to push pending updates to the device or devices.
Push All Pending	Select <i>Push All Pending</i> in the toolbar to push pending updates to all of the devices in the list.
Refresh	Select to refresh the list.
By Package	Displays the service status information by installed package name.
By Device	Displays the service status information by device name.
Search	Use the search field to find a specific device or package in the table.

Service status by Device

When you click the *By Device* button in the toolbar, the *Service Status* page displays a list of all the managed FortiGate devices, their last update time, and their status.

You can pushing pending updates to the devices, either individually or all at the same time. You can refresh the list by clicking *Refresh* in the toolbar.

Device	The device serial number or host name is displayed.
Status	<p>The service update status. A device's status can be one of the following:</p> <ul style="list-style-type: none"> • <i>Up to Date</i>: The latest package has been received by the FortiGate unit. • <i>Never Updated</i>: The FortiGate unit has never requested or received the package. • <i>Pending</i>: The FortiGate unit has an older version of the package due to an acceptable reason (such as the scheduled update time having not come yet). Hover the mouse over a pending icon to view the package to be installed. • <i>Problem</i>: The FortiGate unit missed the scheduled query, or did not correctly receive the latest package. • <i>Unknown</i>: The FortiGate unit's status is not currently known.
Last Update Time	The date and time of the last update.

Service status by Package

When you click the *By Package* button, the *Service Status* page shows a list of all the installed packages, the applicable firmware version, the package version, and the progress on package installation to devices. You can drill-

down to view the installed device list.

The content pane displays the following information:

Installed Packages Name	The name of the installed package.
Applicable Firmware Version	The firmware version of the device for which the installed package is created.
Package Version	The version of the installed package.
Installed Devices	The package installation progress for the devices. Click the <i><number> of <number></i> link to view the installed device list.

To view the installed device list:

1. Go to *FortiGuard > Package Management > Service Status*.
2. In the toolbar, click *By Package*.
The list of installed packages is displayed.
3. In the *Installed Devices* column, click the *<number> of <number>* link for the installed package.
Device details are displayed.

Device Name	The name of the device.
Current Version	The version of the package.
Status	The device update status.
Last Update Time	The time of the last package update.

4. Click the *Back* arrow to return to the previous page.

Query server management

The query server manager shows when updates are received from the server, the update version, the size of the update, and the update history. It also has graphs showing the number of queries from all the managed FortiGate units made to the FortiManager device.

Receive status

To view the received packages, go to *FortiGuard > Query Server Management > Receive Status*.

The following information is displayed:

Refresh	Select to refresh the table.
Search	Use the search field to find a specific entry in the table.
History	The record of received packages.

Package Received	The name of the received package.
Latest Version (Release Date/Time)	The latest version of the received package.
Size	The size of the package.
Update History	Click to view the package update history.

Update history

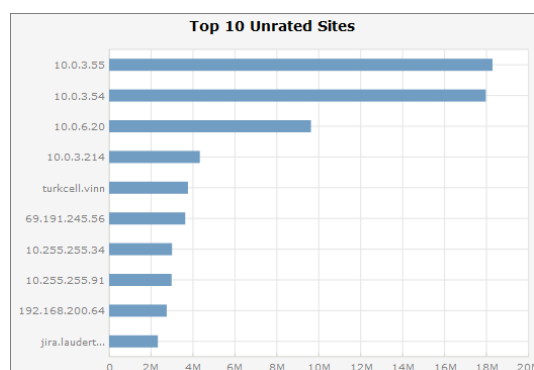
When you click the *Update History* button for a package, the *Update History* pane is displayed for the package.

It shows the update times, the events that occurred, the statuses of the updates, and the versions downloaded.

Query status

Go to *FortiGuard > Query Server Management > Query Status* to view graphs that show:

- The number of queries made from all managed devices to the FortiManager unit over a user selected time period
- The top ten unrated sites
- The top ten devices for a user selected time period



The following information is displayed:

Top 10 Unrated Sites	Displays the top 10 unrated sites and the number of events. Hover the cursor over a row to see the exact number of queries.
Top 10 Devices	Displays the top 10 devices and number of sessions. Hover the cursor over a row to see the exact number of queries. Click a row to see a graph of the queries for that device.
Number of Queries	Displays the number of queries over a period of time.

Firmware images

Go to *FortiGuard > Firmware Images* to manage the firmware images stored on the FortiManager device. You can import firmware images for FortiGate, FortiCarrier, FortiAnalyzer, FortiManager, FortiAP, and FortiExtender.

You can download only those images that are needed from the FDS systems, and customize which firmware images are available for deployment.

The following information and settings are available:

Import Images	Select to open the firmware image import list.
Models	From the dropdown list, select <i>All</i> to show all the available models on the FortiGuard server, or select <i>Managed</i> to show only the models that are currently being managed by the FortiManager device.
Product	Select a managed product type from the dropdown list.
Search	Use the search field to find a specific entry in the table.
Model	The device model number that the firmware is applicable to.
Latest Version (Release Date/Time)	The latest version of the firmware that is available.
Preferred Version	The firmware version that you would like to use on the device. Click <i>Change</i> to open the <i>Change Version</i> dialog box, then select the desired version from the dropdown list and select <i>OK</i> to change the preferred version.
Size	The size of the firmware image.
Status	The status of the image, that is, from where it is available.
Action Status	The status of the current action being taken.
Release Notes	A link to a copy of the release for the firmware image that has been downloaded.
Download/Delete	Download the firmware image from the FDS if it is available. If the firmware images has already been downloaded, then delete the firmware image from the FortiManager device.

For information about upgrading your FortiManager device, see the [FortiManager Release Notes](#) or contact Fortinet Customer Service & Support.

To import a firmware image:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select a device in the list, and click *Import* in the toolbar. The *Firmware Upload* dialog box, opens.
3. Click *Browse* to browse to the desired firmware image file, or drag and drop the file onto the dialog box.
4. Click *OK* to import the firmware image.



Firmware images can be downloaded from the Fortinet Customer Service & Support site at <https://support.fortinet.com/> (support account required).

To delete firmware images:

1. Go to *FortiGuard > Firmware Images*, and click *Import Images* in the toolbar.
2. Select the firmware images you would like to delete.
3. Click *Delete* in the toolbar. A confirmation dialog box appears.
4. Click *OK* to delete the firmware images.

FortiSwitch Manager

The *FortiSwitch Manager* module enables you to centrally manage FortiSwitch templates and VLANs, and monitor FortiSwitch devices that are connected to FortiGate devices. You can configure multiple templates for specific FortiSwitch platforms that can be assigned to multiple devices.

The FortiSwitch Manager module includes the following tabs:

Managed Switches	Displays unauthorized and authorized FortiSwitch devices. You can view, authorize, and edit authorized switches, as well as apply templates to switches.
Monitoring FortiSwitch devices	Monitor FortiSwitch devices with a graphical representation of the connected switches.
FortiSwitch Templates	View, create, and edit FortiSwitch templates and VLANs.

The following steps provide an overview of using centralized FortiSwitch management to configure and install templates:

1. Create FortiSwitch VLANs.
See [FortiSwitch VLANs on page 384](#).
2. Create FortiSwitch templates.
See [FortiSwitch Templates on page 381](#).
3. Assign templates to FortiSwitch devices.
See [Assigning templates to FortiSwitch devices on page 380](#).
4. Install the templates to the devices.
On the *Device Manager* pane, select the FortiGate device that controls the FortiAP device, then select *Install > Install Config* from the toolbar, and follow the prompts in the wizard. See [Configuring a device on page 125](#).

Managed Switches

The *Managed Switches* pane allows you to manage FortiSwitch devices that are controlled by FortiGate devices that are managed by the FortiManager.

FortiSwitch devices, listed in the content pane, are grouped based on the controller that they are connected to.



Additional configuration options and short-cuts are available using the right-click content menu. Right-click on the mouse on different parts of the navigation panes on the GUI page to access these context menus.



If workspace or workflow is enabled, the ADOM must be locked before changes can be made. See [Locking an ADOM on page 64](#).

Go to *FortiSwitch Manager > Managed Switches* to manage FortiSwitch devices. Managed switches are organized by their FortiGate controller.

FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments
fgt102[root]	test	S124DP3X16008011	FortiSwitch-124D-POE	192.168.4.4	S124DP-v3.5.2-build265,170123 (GA)	124-poe	Fri Mar 30 03:47:20 2018	
fgt102[root]		S424DN3X16000142	FortiSwitch-424D	192.168.4.2	S424DN-v3.5.1-build262,161115 (GA)		Fri Mar 30 21:03:59 2018	
fgt102[root]		S524DN4K15000037	FortiSwitch-524D	192.168.4.3	S524DN-v3.5.1-build262,161115 (GA)		Thu Mar 22 01:09:21 2018	
fgt101[root]	248D-POE	S248DP3W16000227	FortiSwitch-248D-POE	192.168.66.8	S248DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:44 2017	
fgt101[root]	424D-FPOE	S424DF3X16000356	FortiSwitch-424D-FPOE	192.168.66.2	S424DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:31 2017	
fgt101[root]	424D-POE	S424DP3X16000162	FortiSwitch-424D-POE	192.168.66.6	S424DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:50 2017	
fgt101[root]	448D	S448DN3X16000287	FortiSwitch-448D	192.168.66.5	S448DN-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:35 2017	
fgt101[root]	524D-FPOE	S524DF4K16000098	FortiSwitch-524D-FPOE	192.168.66.3	S524DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:41 2017	

Quick status bar

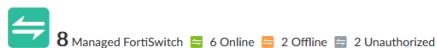
You can quickly view the status of devices on the *Managed Switches* pane by using the quick status bar, which contains the following options:

- Managed FortiSwitch
- Online
- Offline
- Unauthorized

You can click each quick status to display in the content pane only the devices referenced in the quick status.

To view the quick status bar:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiSwitch Manager > Managed Switches*. The quick status bar is displayed above the content pane.



3. In the tree menu, select a FortiGate or *All_FortiGate*. The devices for the group are displayed in the content pane, and the quick status bar updates.
4. Click on each quick status to filter the devices displayed on the content pane. For example, click *Offline*, and the content pane will display only devices that are currently offline.

Managing FortiSwitches

FortiSwitch devices can be managed from the content pane below the quick status bar on the *FortiSwitch Manager > Managed Switches* pane.

FortiGate	FortiSwitch Name	Serial Number	Platform	Connected Via	OS Version	Template	Join Time	Comments
fgt102[root]	test	S124DP3X00000000	FortiSwitch-124D-POE	192.168.0.1	S124DP-v3.5.2-build265,170123 (GA)	124-poe	Fri Mar 30 03:47:20 2018	
fgt102[root]		S424DN3X00000000	FortiSwitch-424D	192.168.0.2	S424DN-v3.5.1-build262,161115 (GA)		Fri Mar 30 21:03:59 2018	
fgt102[root]		S524DN4K00000000	FortiSwitch-524D	192.168.1.1	S524DN-v3.5.1-build262,161115 (GA)		Thu Mar 22 01:09:21 2018	
fgt101[root]	248D-POE	S248DP3W00000000	FortiSwitch-248D-POE	192.168.2.1	S248DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:44 2017	
fgt101[root]	424D-FPOE	S424DF3X00000000	FortiSwitch-424D-FPOE	192.168.1.2	S424DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:31 2017	
fgt101[root]	424D-POE	S424DP3X00000000	FortiSwitch-424D-POE	192.168.2.2	S424DP-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:50 2017	
fgt101[root]	448D	S448DN3X00000000	FortiSwitch-448D	192.168.3.2	S448DN-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:35 2017	
fgt101[root]	524D-FPOE	S524DF4K00000000	FortiSwitch-524D-FPOE	192.168.3.1	S524DF-v3.5.2-build265,170123 (GA)		Tue Mar 14 20:04:41 2017	

The following options are available from the toolbar and right-click menu:

Edit	Edit the selected FortiSwitch.
Delete	Delete the switch or switches.
Assign Template	Assign a template to the switch. Only applicable templates will be listed. See Assigning templates to FortiSwitch devices on page 380 .
Authorize	Authorize an unregistered switch. See Authorizing and deauthorizing FortiSwitch devices on page 379 . This option is also available in the toolbar by selecting <i>More</i> .
Deauthorize	Deauthorize a registered switch. See Authorizing and deauthorizing FortiSwitch devices on page 379 . This option is also available in the toolbar by selecting <i>More</i> .
Restart	Restart the switch. This option is also available in the toolbar by selecting <i>More</i> .
Upgrade	Upgrade the switch. The FortiSwitch must already be authorized. This option is also available in the toolbar by selecting <i>More</i> .
Refresh	Refresh the switch list. This option is also available in the toolbar by selecting <i>More</i> .
Connect to CLI	Connect to FortiSwitch device's CLI, if available. This option is also available in the toolbar by selecting <i>More</i> .
Column Settings	Click to select which columns to display or select <i>Reset to Default</i> to display the default columns. This option is only available in the toolbar.
Search	Enter a search string into the search field to search the switch list. This option is only available in the toolbar.

The following information is available in the content pane:

FortiGate	The FortiGate that the FortiSwitch is connected to.
FortiSwitch Name	The name assigned to the switch.
Serial Number	The serial number of the switch.
Platform	The FortiSwitch model.

Connected Via	The IP address of the switch.
OS Version	The OS version on the switch.
Template	The FortiSwitch template assigned to the device, if any.
Join Time	The date and time that the switch joined.
Comments	User entered comments.

Editing switches

FortiSwitch devices can be edited from the *FortiSwitch Manager > Managed Switches* pane.

To edit FortiSwitch devices:

1. In the tree menu, select the FortiGate that contains the FortiSwitch device to be edited, or select *All_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the content pane.
3. Double-click on the switch, select the switch and click *Edit* from the toolbar, or right-click on the switch and select *Edit*. The *Edit Managed FortiSwitch* window opens.

Edit Managed FortiSwitch

Serial Number: S248DP3W00000000

Name:

Description:

Template:

Managed Switch Status

Status: Connected

Connecting From: 192.168.0.1

Join Time: Tue Mar 14 20:04:44 2017

State: Authorized

Firmware

FortiSwitch OS Version: S248DP-v3.5.2-build265,170123 (GA) [\[Upgrade\]](#)

4. Edit the following options, then click *Apply* to apply your changes.

Serial Number	The device's serial number. This field cannot be edited.
Name	The name of the FortiSwitch.
Description	A description of the FortiSwitch, such as its model.
Template	Select the template that will be applied to the FortiSwitch from the dropdown list. Only applicable templates are available.
Status	The status of the FortiSwitch, such as <i>Connected</i> . Click <i>Restart</i> to restart the switch.
Connecting From	The IP address of the switch.
Join Time	The date and time that the switch joined.

State	<p>The state of the AP, such as <i>Authorized</i>.</p> <p>If the switch is authorized, click <i>De-authorize</i> to deauthorize the switch. If the switch is not authorized, click <i>Authorize</i> to authorize it. See Authorizing and deauthorizing FortiSwitch devices on page 379.</p>
FortiSwitch OS Version	<p>The OS version on the switch.</p> <p>Click <i>Upgrade</i> to upgrade the firmware to a newer version if you have one available. See Firmware Management on page 152</p>

Deleting switches

FortiSwitch devices can be deleted from the *FortiSwitch Manager > Managed Switches* pane.

To delete FortiSwitch devices:

1. In the tree menu, select the FortiGate that contains the switch or switches to be deleted, or select *All_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the list in the content pane.
3. Select the switch or switches that you need to delete.
4. Click *Delete* from the toolbar, or right-click and select *Delete*.
5. Click *OK* in the confirmation dialog box to delete the switch or switches.

Authorizing and deauthorizing FortiSwitch devices

FortiSwitch devices can be authorized and deauthorized from the *Managed Switches* tab, or from the *Edit Managed FortiSwitch* pane (see [Editing switches on page 378](#)).

To authorize FortiSwitch devices:

1. In the tree menu, select FortiGate that contains the unauthorized FortiSwitch devices, or select *All_FortiGate* to list all of the switches.
2. In the quick status bar, click *Unauthorized*. The unauthorized FortiSwitch devices are displayed in the content pane.
3. Select the switches and either click *More > Authorize* from the toolbar, or right-click and select *Authorize*.
4. Select *OK* in the confirmation dialog box to authorize the selected devices.

To deauthorize FortiSwitch devices:

1. In the tree menu, select FortiGate that contains the FortiSwitch devices to be deauthorized
2. Select the FortiSwitch devices and either click *More > Deauthorize* from the toolbar, or right-click and select *Deauthorize*.
3. Select *OK* in the confirmation dialog box to deauthorize the selected devices.

Assigning templates to FortiSwitch devices

You use the FortiSwitch Manager pane to assign templates to switches, and you use the Device Manager pane to install the templates to the switches when you install a configuration to the FortiGate that controls the FortiSwitch device.

For more information about creating and managing FortiSwitch templates, see [FortiSwitch Templates on page 381](#).

To assign a templates:

1. In the tree menu, select the FortiGate that contains the FortiSwitch device the template will be applied to, or select *All_FortiGate* to list all of the switches.
2. Select the appropriate option from the quick status bar, and locate the switch in the content pane.
3. Select the switch and click *Assign Template* from the toolbar, or right-click on the switch and select *Assign Template*. The *Assign FortiSwitch Template* dialog box opens.
4. Select a FortiSwitch template from the dropdown list, then click *OK* to assign it.



Only templates that apply to the specific device model will be available for selection.



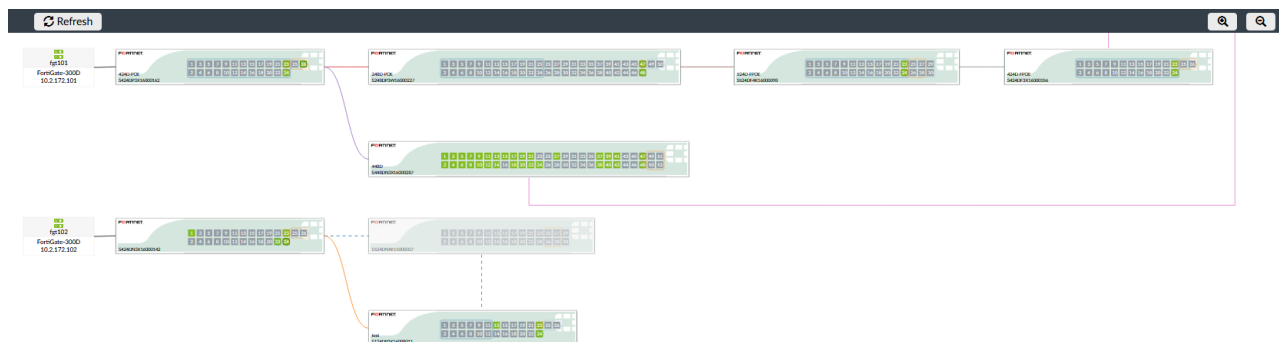
Templates can also be applied when editing a device. See [Editing switches on page 378](#).

To install templates to devices:

1. Go to the *Device Manager* pane.
2. Select the FortiGate device that controls the FortiSwitch
3. Right click and select *Install Config*, or select *Install > Install Config* from the toolbar.
4. Click *OK* in the confirmation dialog box to install the configuration to the device. See [Configuring a device on page 125](#) for more information.

Monitoring FortiSwitch devices

The *FortiSwitch Manager > Monitor* pane shows a graphical representation of the connected FortiSwitch devices.



Ports that are transmitting and receiving data are highlighted in green. Port groups, such as PoE or SFP+ ports, are encircled in different colored boxes.

Hovering the cursor over the edge of a port group will open a pop-up showing the type of port in the group. Hovering the cursor over a port will open a pop-up showing information about the port, including:

Port	The port number.
Peer Device	The device that this switch is connected to. The current port, as well as the port that it is connected to on the connected, and the connection between the two devices, will be highlighted. This item is only displayed when the port is connected to another FortiSwitch device.
Native VLAN	The native VLAN of the port.
PoE	Whether or not the port is currently providing PoE power. This item is only displayed on PoE ports.
Link	The state of the link, either <i>up</i> or <i>down</i> .
Speed	The speed of the port, such as <i>1000Mbps/Full Duplex</i> . The value is <i>0Mbps</i> if the link is down.
Bytes Sent	The total number of bytes sent by the port.
Bytes Received	The total number of bytes received by the port.

FortiSwitch Templates

The *FortiSwitch Manager > FortiSwitch Templates* tab allows you to create and manage FortiSwitch templates and VLANs that can be assigned to FortiSwitch devices.

FortiSwitch templates

FortiSwitch templates define VLAN, and PoE assignments for a FortiSwitch platform.

To view FortiSwitch templates, ensure that you are in the correct ADOM, go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch Templates* in the tree menu.

+ Create New Edit Delete		
Template Name	Platform	
<input type="checkbox"/> 124-poe	FortiSwitch-124D-POE	
<input type="checkbox"/> 248-poe	FortiSwitch-248D-POE	
<input type="checkbox"/> switch-124D	FortiSwitch-124D	

The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch template. See Creating FortiSwitch templates on page 382 .
Edit	Edit the selected template.
Delete	Delete the selected template or templates.
Search	Enter a search string into the search field to search the template list.

To edit a template:

1. Either double-click a template name, right-click a template and select *Edit*, or select a template then click *Edit* in the toolbar. The *Edit FortiSwitch Template* pane opens.
2. Edit the settings as required, then click *OK* to apply your changes.

To delete templates:

1. Select the template or templates that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected template or templates.

Creating FortiSwitch templates

When creating a new FortiSwitch template, the platform must be selected before configuring VLAN assignments.

To create a FortiSwitch template:

1. On the *FortiSwitch Template* pane, click *Create New* in the toolbar. The *Create New FortiSwitch Template* window opens.

Create New FortiSwitch Template

Template Name

Comments

Platforms

FortiSwitch-3632D

Switch VLAN Assignments

+ Add Port + Create Trunk Edit Delete

Port	Native VLAN	Allowed VLAN	POE	DHCP Blocking	IGMP Snooping	Loop Guard	STP
<input type="checkbox"/>	+	+		✓	✓	✗	
<input type="checkbox"/>	+	+		✓	✓	✗	
<input type="checkbox"/>	+	+		✓	✓	✗	

OK

Cancel

2. Enter the following information, then click **OK** to create the new template.

Template Name	Type a name for the template.
Comments	Optionally, enter comments.
Platforms	Select the platform that the template will apply to from the dropdown list.
Switch VLAN Assignments	Configure VLAN assignments. A platform must be selected before VLAN assignments can be configured.
Add Port	Add a port to the table.
Create Trunk	Create a trunk. See To create a trunk group: on page 384 .
Edit	Edit the selected trunk.
Delete	Delete the selected ports or trunks.
Port	Select a port profile from the dropdown list.
Native VLAN	Select the native VLAN from the available VLAN objects. See FortiSwitch VLANs on page 384 .
Allowed VLAN	Select the allowed VLAN from the available VLAN objects. See FortiSwitch VLANs on page 384 .
POE	If applicable, right-click to enable or disable PoE for the port.
DHCP Blocking	Right-click to enable or disable DHCP blocking for the port or trunk. If the port is in a trunk, then DHCP blocking can only be enabled for the trunk, and not the individual ports.
IGMP Snooping	Right-click to enable or disable IGMP snooping for the port or trunk. If the port is in a trunk, then IGMP snooping can only be enabled for the trunk, and not the individual ports.
Loop Guard	Right-click to enable or disable Loop Guard for the port. Loop Guard cannot be applied to trunks, or ports that are in trunks.
STP	Right-click to enable or disable STP for the port or trunk. If the port is in a trunk, then STP can only be enabled for the trunk, and not the individual ports.
Edge Port	Right-click to enable or disable Edge Port for the port or trunk. If the port is in a trunk, then STP can only be enabled for the trunk, and not the individual ports.
STP BPDU Guard	Right-click to enable or disable STP BPDU Guard for the port or trunk. If the port is in a trunk, then STP BPDU Guard can only be enabled for the trunk, and not the individual ports.
STP Root Guard	Right-click to enable or disable STP Root Guard for the port or trunk. If the port is in a trunk, then STP Root Guard can only be enabled for the trunk, and not the individual ports.

To create a trunk group:

1. On the *Create New FortiSwitch Template* pane, click *Create Trunk* in the *Switch VLAN Assignments* toolbar. The *New Trunk Group* dialog box opens.
2. Enter a name for the trunk group in the *Name* field.
3. In the *Members* field, select all the ports that will be in the group from the drop-down list.
4. Select the mode: *lacp-active* (active link aggregation), *lacp-passive* (passive link aggregation), or *static*.
5. Click *OK* to create the trunk group.

FortiSwitch VLANs

VLANs are used when creating FortiSwitch templates.

To view FortiSwitch templates, ensure that you are in the correct ADOM, go to *FortiSwitch Manager > FortiSwitch Templates*, and select *FortiSwitch VLANs* in the tree menu.

+ Create New Edit Delete		
Name		VLAN ID
<input type="checkbox"/> vlan10		10
<input type="checkbox"/> vlan16		16
<input type="checkbox"/> vlan3		3
<input type="checkbox"/> vlan4		4
<input type="checkbox"/> vlan5		5

The following options are available in the toolbar and right-click menu:

Create New	Create a new FortiSwitch VLAN. See Creating FortiSwitch VLANs on page 384 .
Edit	Edit the selected VLAN.
Delete	Delete the selected VLAN or VLANs.
Search	Enter a search string into the search field to search the VLAN list.

To edit a VLAN:

1. Either double-click a VLAN, right-click a VLAN and select *Edit*, or select a VLAN then click *Edit* in the toolbar. The *Edit VLAN Definition* pane opens. The interface name and VLAN ID cannot be edited.
2. Edit the settings as required, then click *OK* to apply your changes.

To delete VLANs:

1. Select the VLAN or VLANs that will be deleted.
2. Either click *Delete* from the toolbar, or right-click and select *Delete*.
3. Click *OK* in the confirmation dialog box to delete the selected VLAN or VLANs.

Creating FortiSwitch VLANs

To create a FortiSwitch VLAN:

1. On the *FortiSwitch VLAN* pane, click *Create New* in the toolbar. The *Create New VLAN Definition* window opens.

Create New VLAN Definition

Interface Name:

VLAN ID:

Role:

Estimated Bandwidth: Kbps Upstream Kbps Downstream

Address

Addressing mode:

IP/Network Mask:

IPv6 Addressing mode:

IPv6 Address/Prefix:

Restrict Access

Administrative Access

<input type="checkbox"/> CAPWAP	<input type="checkbox"/> DNP	<input type="checkbox"/> FGFM
<input type="checkbox"/> FTM	<input type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS
<input type="checkbox"/> PING	<input type="checkbox"/> PROBE-RESPONSE	<input type="checkbox"/> RADIUS-ACCT
<input type="checkbox"/> SNMP	<input type="checkbox"/> SSH	<input type="checkbox"/> TELNET

IPv6 Administrative Access

<input type="checkbox"/> CAPWAP	<input type="checkbox"/> FGFM	<input type="checkbox"/> HTTP
<input type="checkbox"/> HTTPS	<input type="checkbox"/> PING	<input type="checkbox"/> SNMP
<input type="checkbox"/> SSH	<input type="checkbox"/> TELNET	

DHCP Server:

Address Range

+ Create ☒ Edit ☐ Delete ☐

Starting IP	End IP
<input type="checkbox"/> 192.168.0.1	192.168.0.5

Netmask:

Default Gateway:

DNS Server

DNS Server 1:

DNS Server 2:

DNS Server 3:

Advanced...

Networked Devices

Device Detection:

Active Scanning:

Admission Control

Security Mode:

Miscellaneous

Scan Outgoing Connections to Botnet Sites:

Secondary IP Address:

Status

Comments:

Interface State:

Advanced Options

color:

2. Enter the following information, then click **OK** to add the new VLAN.

Interface Name	Enter a name for the interface.
VLAN ID	Enter the VLAN ID
Role	Select the role for the interface: <i>DMZ</i> , <i>LAN</i> , <i>UNDEFINED</i> , or <i>WAN</i> .
Estimated Bandwidth	Enter the estimated upstream and downstream bandwidths. This option is only available when <i>Role</i> is <i>WAN</i> .
Address	
Addressing mode	The addressing mode.
IP/Network Mask	Enter the IP address and netmask.
IPv6 Addressing mode	Select the IPv6 addressing mode: <i>Manual</i> or <i>DHCP</i> .

IPv6 Address/Prefix	Enter the IPv6 address. This option is only available when <i>IPv6 Addressing mode</i> is <i>Manual</i> .
Restrict Access	
Administrative Access	Select the allowed administrative service protocols from: <i>CAPWAP, DNP, FGFM,FTM,HTTP, HTTPS, PING, PROBE-RESPONSE, RADIUS-ACCT, SNMP, SSH, and TELNET</i> .
IPv6 Administrative Access	Select the allowed administrative service protocols from: <i>CAPWAP, FGFM, HTTP, HTTPS, PING, SNMP, SSH, and TELNET</i> .
DHCP Server	Turn the DHCP server on or off. This option is only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i> .
DHCP Server IP	Enter the DHCP server IP address. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Relay</i> .
Address Range	Configure address ranges for DHCP. Click <i>Create</i> to create a new range. Ranges can also be edited and deleted as required. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
Netmask	Enter the netmask. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
Default Gateway	Configure the default gateway: <i>Same as Interface IP</i> , or <i>Specify</i> . If set to <i>Specify</i> , enter the gateway IP address in the field. This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
DNS Server	Configure the DNS server: <i>Same as System DNS</i> , <i>Same as Interface IP</i> , or <i>Specify</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i> .
DNS Server 1 - 3	Enter the DNS server IP addresses. This option is only available when <i>DHCP Server</i> is <i>ON</i> , <i>Mode</i> is <i>Server</i> , and <i>DNS Server</i> is <i>Specify</i> .
Mode	Select the DHCP mode: <i>Server</i> or <i>Relay</i> . This option is only available when <i>DHCP Server</i> is <i>ON</i> .

NTP Server	<p>Configure the NTP server: <i>Local</i>, <i>Same as System NTP</i>, or <i>Specify</i>. If set to <i>Specify</i>, enter the NTP server IP address in the field.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
Time Zone	<p>Configure the timezone: <i>Disable</i>, <i>Same as System</i>, or <i>Specify</i>. If set to <i>Specify</i>, select the timezone from the dropdown list.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
Next Bootstrap Server	<p>Enter the IP address of the next bootstrap server.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
Additional DHCP Options	<p>In the <i>Lease Time</i> field, enter the lease time, in seconds. Default: 604800 seconds (7 days).</p> <p>Add DHCP options to the table. See To add additional DHCP options: on page 389 for details. Options can also be edited and deleted as required.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
MAC Reservation + Access Control	<p>Select the action to take with unknown MAC addresses: <i>assign</i> or <i>block</i>.</p> <p>Add MAC address actions to the table. See To add a MAC address reservation: on page 389 for details. Reservations can also be edited and deleted as required.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i> and <i>Mode</i> is <i>Server</i>.</p>
Type	<p>Select the type: <i>Regular</i>, or <i>IPsec</i>.</p> <p>This option is only available when <i>DHCP Server</i> is <i>ON</i>.</p>
Networked Devices	<p>These options are only available when <i>Role</i> is <i>DMZ</i>, <i>LAN</i>, or <i>UNDEFINED</i>.</p>
Device Detection	<p>Turn device detection on or off.</p>
Active Scanning	<p>Turn active scanning on or off.</p> <p>This option is only available when <i>Device Detection</i> is on.</p>
Admission Control	<p>These options are only available when <i>Role</i> is <i>LAN</i> or <i>UNDEFINED</i>.</p>
Security Mode	<p>Select the security mode: <i>CAPTIVE-PORTAL</i>, or <i>NONE</i>.</p>

Authentication Portal	Configure the authentication portal: <i>Local</i> or <i>External</i> . If <i>External</i> is selected, enter the portal in the field. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
User Access	Select <i>Restricted to Groups</i> or <i>Allow All</i> . This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
User Groups	Select user groups from the available groups. This option is available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> and <i>User Access</i> is <i>Restricted to Groups</i> .
Exempt Sources	Select sources that are exempt from the available firewall addresses. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
Device	Select user devices, device categories, and/or device groups. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
Exempt Destinations	Select destinations that are exempt from the available firewall addresses. This option is only available when <i>Security Mode</i> is <i>CAPTIVE-PORTAL</i> .
Exempt Services	Select services that are exempt from the available firewall services. This option is only available when <i>Security mode</i> is <i>CAPTIVE-PORTAL</i> .
Miscellaneous	
Scan Outgoing Connections to Botnet Sites	Select <i>Block</i> , <i>Disable</i> , or <i>Monitor</i> .
Secondary IP Address	Turn secondary IP addresses on or off. Add IP addresses to the table. See To add a secondary IP address: on page 389 for details. Addresses can also be edited and deleted as required.
Status	
Comments	Optionally, enter comments.
Interface State	Select if the interface is <i>Enabled</i> or <i>Disabled</i> .
Advanced Options	
color	Change the color of the interface to one of the 32 options.

To add additional DHCP options:

1. Click *Create* in the *Additional DHCP Options* table toolbar. The *Additional DHCP Options* dialog box opens.

Additional DHCP Options

Option Code: 0

Type: **hex** | ip | string

Hexadecimal Value:

OK Cancel

2. Enter the *Option Code*.
3. Select the *Type*: *hex*, *ip*, or *string*.
4. Enter the corresponding value.
5. Click *OK* to create the option.

To add a MAC address reservation:

1. Click *Create* in the *MAC Reservation + Access Control* table toolbar. The *MAC Reservation + Access Control* dialog box opens.

MAC Reservation + Access Control

MAC Address: 00:00:00:00:00:00

End IP: **Assign IP** | Block | **Reserve IP**

0.0.0.0

Description: 0/255

OK Cancel

2. Enter the *MAC Address*.
3. Select the *End IP*: *Assign IP*, *Block*, or *Reserve IP*. If reserving the IP address, enter it in the field.
4. Optionally, enter a description.
5. Click *OK* to create the reservation.

To add a secondary IP address:

1. Click *Create* in the *Secondary IP address* table toolbar. A dialog box opens.
2. Enter the IP address and netmask in the *IP/Network Mask* field.
3. Select the allowed administrative service protocols from: *CAPWAP*, *DNP*, *FGFM*, *FTM*, *HTTP*, *HTTPS*, *PING*, *PROBE-RESPONSE*, *RADIUS-ACCT*, *SNMP*, *SSH*, and *TELNET*.
4. Click *OK* to add the address.

FortiAnalyzer Features

FortiAnalyzer features can be enabled either for a FortiManager unit or for managed FortiAnalyzer units, but not for both at the same time. The features can be used to view and analyze logs from devices with logging enabled that are managed by the FortiManager.

When the features are enabled manually, logs are stored and FortiAnalyzer features are configured on the FortiManager.

When the features are enabled by adding a FortiAnalyzer to the FortiManager, logs are stored and log storage settings are configured on the FortiAnalyzer device. Managed devices with logging enabled send logs to the FortiAnalyzer. The FortiManager remotely accesses logs on the FortiAnalyzer unit and displays the information. See [Adding FortiAnalyzer devices on page 119](#).

When FortiAnalyzer features are enabled, the following modules are available:

FortiView	View summaries of log data. For example, you can view top threats to your network, top sources of network traffic, top destinations of network traffic and so on. See FortiView on page 393 .
NOC	View multiple panes of network activity, including monitoring network security, WiFi security, and system performance. See NOC on page 406
Log View	View log messages from managed devices with logging enabled. You can view the traffic log, event log, or security log information. See Log View on page 412 .
Event Management	View events from logs that you want to monitor. You can specify what log messages to display as events by configuring event handlers. See Event Management on page 424 .
Reports	Generate reports of data from logs. See Reports on page 441 .

When FortiAnalyzer features are manually enabled, the following options are available on the *System Settings* module:

Dashboard widgets	The following widgets can be added to the dashboard: <i>Log Receive Monitor</i> , <i>Insert Rate vs Receive Rate</i> , <i>Log Insert Lag Time</i> , <i>Receive Rate vs Forwarding Rate</i> , and <i>Disk I/O</i> . The <i>License Information</i> widget will include a <i>Logging</i> section. See Dashboard on page 473 .
Logging Topology	View the logging topology. See Logging Topology on page 487 .
Storage Info	View and configure log storage policies. This pane is only available when ADOMs are enabled.
Fetcher Management	Configure log fetching. See Fetcher Management on page 501 .
Device Log Settings	Configure device log file size, log rolling, and scheduled uploads to a server. See Device logs on page 522 .

File Management

Configure the automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time. See [File Management on page 526](#).

Various other settings and information will be included on the FortiManager when FortiAnalyzer features are enabled.

Enable or disable FortiAnalyzer features

If FortiAnalyzer features are enabled, you cannot add a FortiAnalyzer units to the FortiManager. If a FortiAnalyzer is added to the FortiManager, FortiAnalyzer features are automatically enabled to support the managed FortiAnalyzer unit, and cannot be disabled.

See [Adding FortiAnalyzer devices on page 119](#) for more information.

To enable or disable the FortiAnalyzer features from the GUI:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the *FortiAnalyzer Features* toggle switch.
The FortiManager will reboot to apply the change.

To enable or disable the FortiAnalyzer features from the CLI:

1. Log in to the FortiManager CLI.
2. Enter the following commands:

```
config system global
    set faz-status {enable | disable}
end
```



The FortiAnalyzer feature set is not available on the FortiManager 100C.

Viewing policy rules

When a FortiAnalyzer is managed by a FortiManager, you can view the logs that the FortiAnalyzer unit receives. In the *Log View* module, you can also view the policy rules by clicking a policy ID number.

See [Adding FortiAnalyzer devices on page 119](#).

To view policy rules:

1. Go to *Log View > Traffic*.
2. Click the number in the *Policy ID* column.
The *View Policy* window is displayed, showing the policy rules.

3. Click *Return* to close the window.

FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

FortiView allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity such as user uploads/downloads or videos watched on YouTube on a network-wide user group or on an individual-user level. It presents information in both text and visual format.



This pane is only available when the FortiAnalyzer features are enabled. For more information, see [FortiAnalyzer Features on page 390](#).

You can view summaries of log data in *FortiView* such as top threats to your network, top sources of network traffic, and top destinations of network traffic. Depending on which summary you are viewing, you can view summary information in different formats: table, bubble, map, or tile. For each summary view, you can drill down to see more details.

FortiGate, FortiCarrier, and FortiClient EMS devices support FortiView.

How ADOMs affect the FortiView pane

When ADOMs are enabled, each ADOM has its own data analysis in *FortiView*.

Logs used for FortiView

FortiView displays data from Analytics logs. Data from Archive logs is not displayed in *FortiView*.

FortiView summary list and description

FortiView summaries for FortiGate and FortiCarrier devices

Category	View	Description
Summary	An overview	An overview of most used <i>FortiView</i> summary views. You can select which widgets to display in the <i>Summary</i> .

Category	View	Description
Threats	Top Threats	<p>Lists the top threats to your network.</p> <p>The following incidents are considered threats:</p> <ul style="list-style-type: none"> • Risk applications detected by application control. • Intrusion incidents detected by IPS. • Malicious web sites detected by web filtering. • Malware/botnets detected by antivirus. <p>Note: If FortiGate is running FortiOS 5.0.x, turn on <i>Security Profiles > Client Reputation</i> to view entries in Top Threats.</p>
	Threat Map	<p>Displays a map of the world that shows the top traffic destination country by color. Threats are displayed when the level is equal to or greater than warning and the source IP is a public IP address.</p> <p>The list of threats at the bottom shows the location, threat, severity, and time of the attacks. The color gradient of the darts on the map indicate the traffic risk, where red indicates the more critical risk.</p> <p>This view has no filtering options. See also Viewing the threat map on page 401.</p>
	Indicators of Compromise (IOC)	<p>Displays end users with suspicious web use compromises, including end users' IP addresses, overall threat rating, and number of threats.</p> <p>Note: To use this feature:</p> <ol style="list-style-type: none"> 1. UTM logs of the connected FortiGate devices must be enabled. 2. The FortiManager must subscribe to FortiGuard to keep its threat database current.
Traffic	Top Sources	Displays the highest network traffic by source IP address and interface, device, threat score (blocked and allowed), sessions (blocked and allowed), and bytes (sent and received).
	Top Destinations	Displays the highest network traffic by destination IP addresses, the applications used to access the destination, sessions, and bytes.
	Top Countries	Displays the highest network traffic by country in terms of traffic sessions, including the destination, threat score, sessions, and bytes.
	Policy Hits	Lists the policy hits by policy, device name, VDOM, number of hits, bytes, and last used time and date.

Category	View	Description
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, number of clients, sessions blocked and allowed, and bytes sent and received. For a usage example, see Finding application and user information on page 404 .
	Top Cloud Applications	Displays the top cloud applications used on the network.
	Top Websites	Displays the top allowed and blocked web sites on the network. You can view information by domain or category by using the options in the top right of the toolbar.
	Top Browsing Users	Displays the top web-browsing users, including source, group, number of sites visited, browsing time, and number of bytes sent and received.
VPN	SSL & Dialup IPsec	Displays the users who are accessing the network by using the following types of security over a virtual private network (VPN) tunnel: secure socket layers (SSL) and Internet protocol security (IPsec).
	Site-to-Site IPsec	Displays the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network.
WiFi	Rogue APs	Displays the service set identifiers (SSID) of unauthorized WiFi access points on the network.
	Authorized APs	Displays the names of authorized WiFi access points on the network.
	Authorized SSIDs	Displays the service set identifiers (SSID) of authorized WiFi access points on the network.
	WiFi Clients	Lists the names and IP addresses of the devices logged into the WiFi network.
System	Admin Logins	Displays the users who logged into the managed device.
	System Events	Displays events on the managed device.
	Resource Usage	Displays device CPU, memory, logging, and other performance information for the managed device.
	Failed Authentication Attempts	Displays the IP addresses of the users who failed to log into the managed device.

Category	View	Description
Endpoints	All Endpoints	Lists the FortiClient endpoints registered to the FortiGate device.
	Top Vulnerabilities	Displays vulnerability information about the FortiClient endpoints registered to specific FortiGate devices. View by <i>Device</i> or <i>Vulnerability</i> . In <i>Device</i> view, the table shows the device, source, number and severity of vulnerabilities, and category. In <i>Vulnerability</i> view, select table or bubble format. The table format shows the vulnerability name, severity, category, CVE ID, and host count. The bubble graph format shows vulnerability by severity and frequency.
	Top Threats	Displays the top threats for registered FortiClient endpoints, including the threat, threat level, and the number of incidents (blocked and allowed).
	Top Applications	Displays the top applications used by registered FortiClient endpoints, including the application name, risk level, sessions blocked and allowed, and bytes sent and received.
	Top Web Sites	Displays the top allowed and blocked web sites on the network.

FortiView summaries for FortiClient EMS devices

Category	View	Description
Threats	Top Threats	Lists the top users involved in incidents and the top threats to your network. The following incidents are considered threats: <ul style="list-style-type: none"> • Risk applications detected by application control • Malicious web sites detected by web filtering • Malware/botnets detected by antivirus
Applications & Websites	Top Applications	Displays the top applications used on the network including the application name, category, risk level, number of clients, sessions blocked and allowed, and bytes sent and received.
	Top Websites	Displays the top allowed and blocked web sites on the network.
Endpoints	All Endpoints	Lists the FortiClient endpoints registered to the FortiClient EMS device.
	Top Vulnerabilities	Displays vulnerability information about the FortiClient endpoints that are registered to the FortiClient EMS device. View by <i>Device</i> or <i>Vulnerability</i> . In <i>Device</i> view, the table shows the device, source, number and severity of vulnerabilities, and category. In <i>Vulnerability</i> view, select table or bubble format. The table format shows the vulnerability name, severity, category, CVE ID, and host count. The bubble graph format shows vulnerability by severity and frequency.

Using FortiView

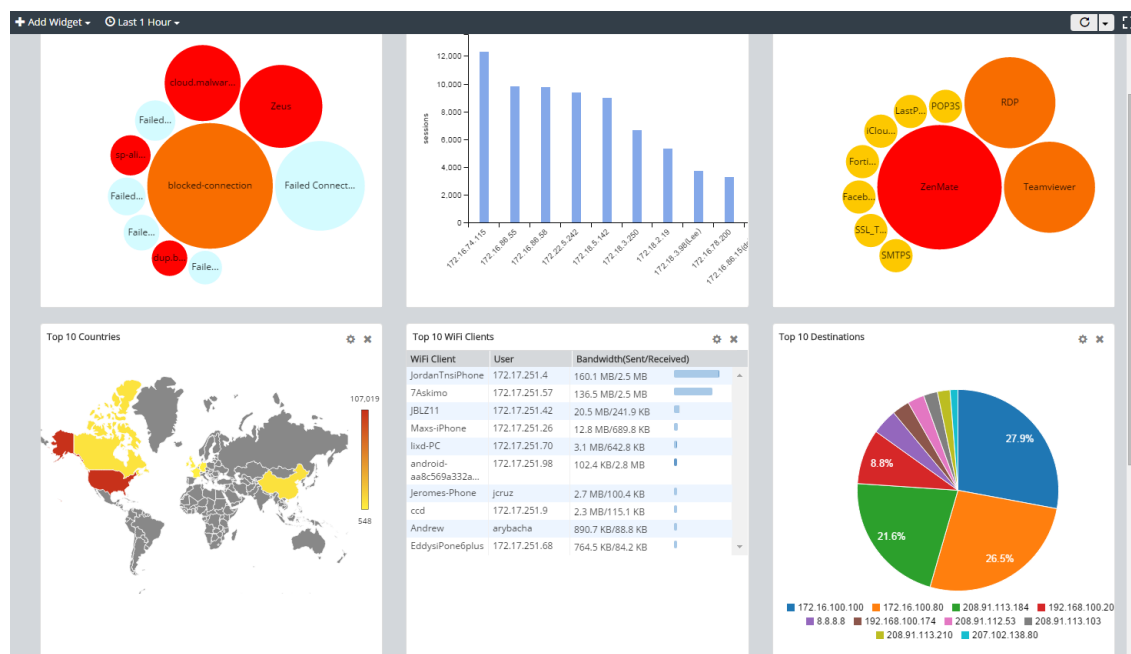
When ADOMs are enabled, *FortiView* displays information for each ADOM so ensure you are in the correct ADOM. See [Switching between ADOMs on page 37](#).

FortiView Summary

The *FortiView Summary* shows you an overview of the most used summary views. You can configure the overall view of the *Summary*.

Each summary view is a widget. You can configure the view settings of each widget, including adding the same widget multiple times, each showing a different view. For example, you can add two Top Threats widgets: one showing the Top 10 Threats view in a bubble chart, and the other showing the Top 20 Threats in a table.

To view the details of each summary view, you can drill down each summary view or use the tree menu to see an individual view.

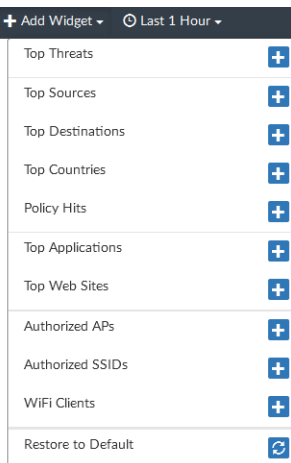


Configuring the overall view settings of the Summary

To add a widget to the Summary:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView*.

3. In the content pane toolbar, click *Add Widget* and select a FortiView summary from the list.



To remove a widget from the Summary:

Click the *Remove This Widget* button in the top-right of the widget.

To specify a time period for all the views on the Summary:

On the *FortiView Summary*, select a time period from the *time period* dropdown list in the toolbar.

To refresh the view and/or set refresh rate:

On the *FortiView Summary*, click the *Refresh Now* button in the toolbar or select a refresh rate from the dropdown menu.

To switch to full-screen mode:

On the *FortiView Summary*, click the *Full Screen* button in the toolbar. To exit full-screen mode, either press *Esc* or click the *Exit Full Screen* button in the top-right.

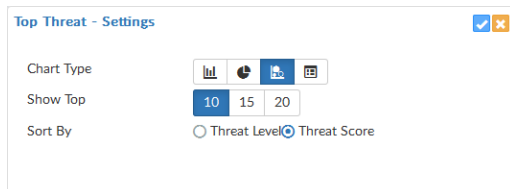
Viewing each widget on the Summary

You can view and drill down each summary view on the *Summary* or you can view an individual page that you access through the tree menu. See [Filtering FortiView summaries on page 402](#).

Configuring the view settings for an individual widget

To Configure the view settings of an individual widget:

1. On the *FortiView Summary*, click the *Edit Settings* button in the top-right of the widget. The summary view flips to the settings panel.



2. On the settings panel, configure the settings for the widget, such as *Chart Type*, *Show Top*, and *Sort By*.
3. Click *OK* in the top-right corner to save the changes.

Viewing FortiView summaries

When viewing summaries, use the controls in the toolbar to select a display format, select a device, specify a time period, refresh the view, set the refresh rate, export the information, and switch to full-screen mode.

Depending on which summary you are viewing, you can view summary information in different formats such as table, bubble, map, or tile.

Some summary views support only one format. For example, *Threat Map* only supports the map format and *Policy Hits* supports only the table format.

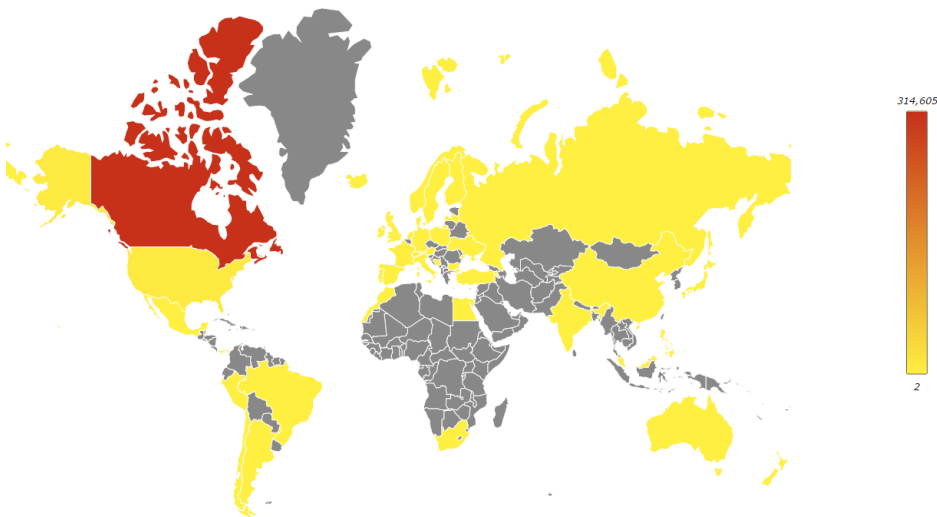
- In summary views that support multiple formats, click the format icon in the top-right to select another format.
- In simple format:
 - To select which items to display, use the *Sort By* dropdown list in the top-left.
- In table format:
 - To select how many items to display, use the *Show* dropdown list in the bottom-right.
 - To sort by a column, click the column title.

Viewing a map of top countries

You can view a map of the *Traffic > Top Countries* summary view. The map shows the destination country.

To view a map of top countries:

1. Go to *FortiView > Traffic > Top Countries*.
2. Select the *Map* icon from the dropdown list in the top-right.



3. Choose a sort method from the *Sort By* list in the top-right.
4. To view more information, hover the mouse over the map.
5. To drill down to view more details, click a country to view details about different dimensions in different tabs.
6. You can continue drilling down by double-clicking an entry.
7. Click the *Back* button in the toolbar to return to the previous view.

Viewing the threat map

You can view an animated world map that displays threats from unified threat management logs. Threats are displayed in real-time. No replay or additional details are available.



You must specify the longitude and latitude of the device to enable threats for the device to display in the threat map. You can edit the device settings to identify the geographical location of the device in *Device Manager*.



To view the threat map:

1. Go to *FortiView > Threats > Threat Map*.
2. In the map, view the geographic location of the threats.
3. In the *Threat Window*, view the threat, level, and location.

Filtering FortiView summaries

Filter *FortiView* summaries using the *Add Filter* box in the toolbar or by right-clicking an entry and selecting a context-sensitive filter. You can also filter by specific devices or log groups and by time.

To filter FortiView summaries using filters in the toolbar:

1. Specify filters in the *Add Filter* box.
 - Regular Search: In the selected summary view, click *Add Filter* and select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters and connect them with “and” or “or”.
 - Advanced Search: Click the *Switch to Advanced Search* icon  at the right end of the *Add Filter* box. In Advanced Search mode, enter the search criteria (log field names and values). Click the *Switch to Regular Search* icon  to go back to regular search.
2. In the *Device* list, select a device.
3. In the *Time* list, select a time period.
4. If necessary, click *Go*.

To filter FortiView summaries using the right-click menu:

In the selected summary view, right-click an entry and select a filter criterion (*Search <filter value>*).

Depending on the column in which your mouse is placed when you right-click, *FortiView* uses the column value as the filter criteria. This context-sensitive filter is only available for certain columns.

Viewing related logs

You can view the related logs for a *FortiView* summary in *Log View*. When you view related logs, the same filters that you applied to the *FortiView* summary are applied to the log messages.

To view related logs for a *FortiView* summary, right-click the entry and select *View Related Logs*.

Exporting filtered summaries

You can export filtered *FortiView* summaries or any level of the drilldowns to PDF and report charts. Filtered summaries are always exported in table format.

To export a filtered summary:

1. In the filtered summary view or its drilldown, click the *Export* button in the top-right and select *Export to PDF* or *Export to Report Chart*.
2. In the dialog box, review and configure settings:
 - Specify a file name for the exported file.
 - In the *Top* field, specify the number of entries to export.
 - If you are in a drilldown view, the tab you are in is selected by default. You can select more tabs. If you are exporting to report charts, the export creates one chart for each tab.
3. Click *OK*.

Charts are saved in the Chart Library. You can use them in the same way you use other charts.



Only log field filters are exported. Device and time period filters are not exported.

FortiView Indicators of Compromise

The *Indicators of Compromise* (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, last detected date, host name, OS, a *Map View*, and number of threats. You can drill down to view threat details.

FortiAnalyzer generates the *Indicators of Compromise* by checking the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. When the check is complete, FortiAnalyzer aggregates all the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise.



To use this Indicators of Compromise summary, you must turn on the UTM web filter of FortiGate devices. You must also subscribe your FortiManager unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See [Subscribing FortiManager to FortiGuard on page 403](#).

Viewing Indicators of Compromise information

Indicators of Compromise information is in *FortiView > Threats > Indicators of Compromise*.

When viewing Indicators of Compromise, use the controls in the toolbar to select *Table* or *Tile* format, select devices, specify a time period, refresh the view, set the refresh rate, export the information, and switch to full-screen mode.

In tile format, you can view a map of the Indicators of Compromise by clicking *Map View* in the tile. To see more details, hover the cursor over a destination

To acknowledge the Indicators of Compromise of an end user, click *Ack*.

To filter entries, click *Add Filter* and specify devices or a time period.

To drill down and view threat details, double-click a tile or a row.

Subscribing FortiManager to FortiGuard

Your FortiManager needs to subscribe to FortiGuard to keep its threat database up to date. You must purchase a FortiGuard Indicators of Compromise Service license for that.

To subscribe FortiManager to FortiGuard:

1. Go to *System Settings > Dashboard*.
2. In the *License Information* widget, find the *FortiGuard > Indicators of Compromise Service* field and click *Purchase*.

Monitoring resource usage of devices

You can monitor how much FortiManager system resources (e.g., CPU, memory, and disk space) each device uses. When ADOMs are enabled, this information is displayed per ADOM. In a specific ADOM, you can view the resource usage information of all the devices under the ADOM.

Go to *FortiView > System > Resource Usage* to monitor resource usage for devices.

Examples of using FortiView

You can use FortiView to find information about your network. The following are some examples.

Finding application and user information

Company ABC has over 1000 employees using different applications across different divisional areas, including supply chain, accounting, facilities and construction, administration, and IT.

The administration team received a \$6000 invoice from a software provider to license an application called Widget-Pro. According to the software provider, an employee at Company ABC is using Widget-Pro software.

The system administrator wants to find who is using applications that are not in the company's list of approved applications. The administrator also wants to determine whether the user is unknown to FortiGuard signatures, identify the list of users, and perform an analysis of their systems.

To find application and user information:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView > Applications & Websites > Top Applications*.
3. Click *Add Filter*, select *Application*, type *Widget-Pro*, and click *Go*.
4. If you do not find the application in the filtered results, go to *Log View > Traffic*.
5. Click the *Add Filter* box, select *Source IP*, type the source IP address, and click *Go*.

Finding unsecured wireless access points

AAA Electronics has multiple access points in their stores for their wireless point-of-sale and mobile devices the sales team uses.

War-driving hackers found an unsecured wireless connection in the AAA Electronics network. Hackers were able to connect to the network and install a program for stealing personal data.

The network administrator already monitors unknown applications using FortiManager alerts and was informed an unauthorized program had been installed. Following an investigation, the administrator determined the program secured a wireless access point. The administrator now wants to determine if any of the other AAA Electronics stores has insecure access points.

To find information on unsecured wireless access points:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView > WiFi > Rogue APs* to view the list of unsecured wireless or rogue access points.

Analyzing and reporting on network traffic

A new administrator starts at #1 Technical College. The school has a free WiFi for students on the condition that they accept the terms and policies for school use.

The new administrator is asked to analyze and report on the top source and destinations students visit, the source and destinations that consume the most bandwidth, and the number of attempts to visit blocked sites.

To review the source and destination traffic and bandwidth:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView > Traffic > Top Sources*.
3. Go to *FortiView > Traffic > Top Destinations*.

Viewing vulnerabilities with high severity and frequency

A-One Company experiences many network vulnerabilities but most of them are of low to medium severity and occur infrequently. The network administrator wants to quickly see which vulnerabilities have high severity and frequency.

To view vulnerabilities with high severity and frequency:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *FortiView > Endpoints > Top Vulnerabilities*.
3. In the toolbar, select *Vulnerability* and *Bubble* format.

Focus on the top right of the bubble chart which shows vulnerabilities with the highest severity and frequency. Hover the cursor over a vulnerability to see additional information and click a vulnerability to drill down to view more details.

NOC

Use the NOC (Network Operations Center) or SOC (Security Operations Center) to view multiple panes of network activity, including monitoring network security, WiFi security, and system performance.

NOC displays both real-time monitoring and historical trends. This centralized monitoring and awareness help you to effectively monitor network events, threats, and security alerts.

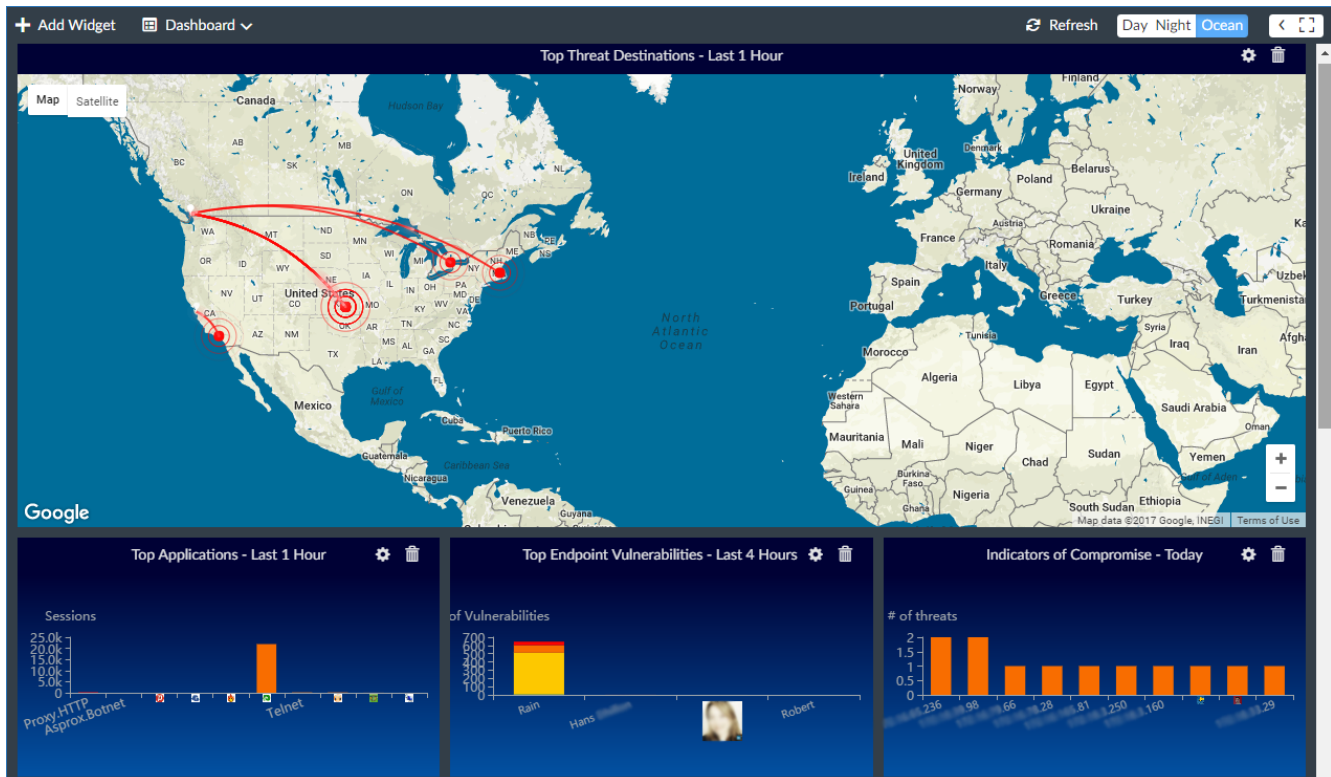


This pane is only available when the FortiAnalyzer features are enabled. For more information, see [FortiAnalyzer Features](#) on page 390.

NOC Dashboard

NOC includes predefined [Security Monitor](#), [WiFi Monitor](#), and [System Performance](#) dashboards.

You can create custom dashboards and add widgets to them. Each pane or widget monitors one activity. You can select what widgets to display, customize widgets, move and resize widgets, and display widgets in full screen or on different monitors.



A good way to use dashboards is to use multiple monitors to display different widgets that show a comprehensive view of your network and security operations in real time. Select widgets that display information most relevant to you.

One scenario is to use the main monitors in the middle to display widgets in a bigger size. These widgets monitor network information that is most important to you. Then use the monitors on the sides to display other information in smaller widgets.

For example, use the top monitor in the middle to display the *Top Threat Destinations* widget in full screen, use the monitor(s) below that to display other *Security Monitor* widgets, use the monitors on the left to display *WiFi Monitor* widgets at the top and *System Performance* widgets at the bottom, and use the monitors on the right as a workspace to display widgets showing the busiest network activity. You can move, add, or remove widgets.

Using the NOC dashboard

NOC dashboards contains widgets that provide network and security information. Use the controls in the dashboard toolbar to work with a dashboard.

Add Widget	Add widgets to a predefined or custom dashboard. For details, see Customizing the NOC dashboard on page 408 .
Dashboard	Create a new dashboard or reset a predefined dashboard to its default settings. For custom dashboards, you can rename or delete the custom dashboard. For details, see Customizing the NOC dashboard on page 408 .
Create New	Create a new dashboard.
Reset	Reset the dashboard.
Select Security Fabric	Select the Security Fabric to display in the dashboard. You need to create a Security Fabric group in FortiGate and add the Security Fabric group in FortiAnalyzer to be able to select a Security Fabric option in the NOC dashboard.
Refresh	Refresh the data in the widgets.
Background color	Change the background color of the dashboard to make widgets easier to view in different room lighting. <ul style="list-style-type: none"> • <i>Day</i> shows a brighter gray background color. • <i>Night</i> shows a black background. • <i>Ocean</i> shows a blue background color.
Hide Side-menu and Show Side-menu	Hide or show the tree menu on the left.
Full Screen	Display in full screen. To exit full screen, press <i>Esc</i> .

Use the controls in the widget title bar to work with widgets.

Settings icon	Change the settings of the widget. Widgets have settings applicable to that widget, such as how many of the top items to display, <i>Time Period</i> , <i>Refresh Interval</i> , and <i>Chart Type</i> .
----------------------	--

View different chart types	Some widget settings let you choose different chart types such as the <i>Disk I/O</i> and <i>Top Countries</i> widget. You can add these widgets multiple times and set each widget to show a different chart type.
Hide or show a data type	For widgets that show different data types, click a data type in the title bar to hide or show that data type in the graph. For example, in the <i>Insert Rate vs Receive Rate</i> widget, click <i>Receive Rate</i> or <i>Insert Rate</i> in the title bar to hide or show that data. In the <i>Disk I/O</i> widget, click <i>Read</i> or <i>Write</i> in the title bar to hide or show that data type.
Remove widget icon	Delete the widget from a predefined or custom dashboard.
Move widget	Click and drag a widget's title bar to move it to another location.
Resize widget	Click and drag the resize button in the bottom-right of the widget.
View more details	Hover the cursor over a widget's data points to see more details.
View a narrower time period	Some widgets have buttons below the graph. Click and drag the buttons to view a narrower time period.
Zoom in and out	For widgets that show information on a map such as the <i>Top Threat Destinations</i> widget, use the scroll wheel to change the zoom level. Click and drag the map to view a different area.

Customizing the NOC dashboard

You can add any widget to a predefined dashboard. You can also move, resize, or delete widgets. You cannot rename or delete a predefined dashboard. To reset a predefined dashboard to its default settings, click *Dashboard > Reset*.

You can add the same widget multiple times and configure each one differently, such as showing a different *Time Period*, *Refresh Interval*, or *Chart Type*.

To create a dashboard:

1. In the toolbar, click *Dashboard > Create New*.
2. Specify the *Name* and whether you want to create a blank dashboard or use a template.
If you select *From Template*, specify which predefined dashboard you want to use as a template.
3. Click *OK*. The new dashboard appears in the tree menu.

To display Security Fabric in NOC:

1. Create a Security Fabric in FortiGate.
2. Add the Security Fabric in FortiAnalyzer.
3. Go to *NOC > Dashboard > Select Security Fabric*. The *Add Device* dialog box will open.
4. Select the Security Fabric you want to display in the NOC Dashboard.
5. Add desired widgets to the dashboard.

To add a widget:

1. Select the predefined or custom dashboard where you want to add a widget.
2. Click *Add Widget* to expand the menu; then locate the widget you want to add.
3. Click the + button to add widgets.
4. When you have finished adding widgets, click the close button to close the *Add Widget* pane.

NOC dashboards and widgets

NOC includes the following predefined dashboards and widgets. You can create custom dashboards and add any widget to any predefined or custom dashboard.

Security Monitor

The Security Monitor dashboard includes the following widgets:

Top Threat Destinations	A world map showing the highest network traffic. Hover the cursor over data points to see the source device and IP address, destination IP address and country, threat level, and the number of incidents (blocked and allowed).
Top Threat	<p>The top threats to your network. Hover the cursor over data points to see the threat, category, threat level, threat score (blocked and allowed), and the number of incidents (blocked and allowed).</p> <p>The following incidents are considered threats:</p> <ul style="list-style-type: none"> • Risk applications detected by application control • Intrusion incidents detected by IPS • Malicious web sites detected by web filtering • Malware/botnets detected by antivirus
Top Applications	The top applications used on the network. Hover the cursor over data points to see the application name, risk level, category, sessions (blocked and allowed), and bytes (sent and received).
Indicators of Compromise	Suspicious web use compromises. Hover the cursor over data points to see the end user IP address, host name, group, OS version, threat level, number of threats, and blacklist count.
Top Endpoint Vulnerabilities	Vulnerability information about FortiClient endpoints. Hover the cursor over data points to see the vulnerability count (critical, high, medium, and low), source IP address and device, and category.
Top Sources	The highest network traffic by source IP address and interface, sessions (blocked and allowed), threat score (blocked and allowed), and bytes (sent and received).
Top Countries	The highest network traffic by country, sessions (blocked and allowed), and bytes (sent and received). You can display this widget as a treemap chart, bubble chart, or bar chart; sorted by bandwidth or the number of sessions.

Security Fabric Score Summary	Total score and suggested actions to improve the score.
Historical Security Fabric Scores	Changes of the audit score over time.
Security Fabric Topology	A topology map showing the logical structure of connected security fabric devices.
Top Dialup VPN	A world map showing the users accessing the network using SSL or IPsec over a VPN tunnel. Hover the cursor over data points to see the user name or IP address, connected from IP address and country, connection time and duration, and bytes (sent and received).
VPN Site-to-Site	A world map showing the names of VPN tunnels with Internet protocol security (IPsec) that are accessing the network. Hover the cursor over data points to see the site-to-site IPsec tunnel, connected from and to IP address (including city and country if available), duration, and bytes (sent and received).
FortiSandbox - Scanning Statistics	The number of files scanned by FortiSandbox. This chart shows the files by type: malicious, suspicious, clean, and others. Hover the cursor over data points to see the number of files of each type.
FortiSandbox - Top Malicious & Suspicious File Users	Users or IP addresses that have the highest number of malicious and suspicious files detected by FortiSandbox. This chart shows the username and avatar if it's available, otherwise it shows the IP address. Hover the cursor over data points to see the number of files.

WiFi Monitor

The WiFi dashboard includes the following widgets:

Authorized APs	A world map showing the names of authorized WiFi access points on the network.
Top SSID	The top SSID (service set identifiers) of authorized WiFi access points on the network. Hover the cursor over data points to see the SSID and bytes (sent and received).
Top Rogue APs	The top SSID (service set identifiers) of unauthorized WiFi access points on the network. Hover the cursor over data points to see the SSID and total live time.

System Performance

The System Performance dashboard includes the following widgets:

CPU & Memory Usage	The usage status of the CPU and memory.
Multi-Core CPU Usage	The usage status of a multi-core CPU.

Insert Rate vs Receive Rate	<p>The number of logs received vs the number of logs actively inserted into the database, including the maximum and minimum rates.</p> <ul style="list-style-type: none">• Receive rate: how many logs are being received.• insert rate: how many logs are being actively inserted into the database. <p>If the insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.</p>
Receive Rate vs Forwarding Rate	<p>The number of logs received vs the number of logs forwarded out, including the maximum and minimum rates.</p> <ul style="list-style-type: none">• Receive rate: how many logs are being received.• Forward rate: how many logs are being forwarded out.
Disk I/O	<p>The disk <i>Transaction Rate</i> (I/Os per second), <i>Throughput</i> (KB/s), or <i>Utilization</i> (%). The <i>Transaction Rate</i> and <i>Throughput</i> graphs also show the maximum and minimum disk activity.</p>

Log View

You can view log information by device or by log group.



When rebuilding the SQL database, *Log View* is not available until the rebuild is complete. Click the *Show Progress* link in the message to view the status of the SQL rebuild.



This pane is only available when the FortiAnalyzer features are enabled. For more information, see [FortiAnalyzer Features on page 390](#).

When ADOMs are enabled, each ADOM has its own information displayed in *Log View*.

Log View displays log messages from Analytics logs and Archive logs:

- Historical logs and real-time logs in *Log View* are from Analytics logs.
- *Log Browse* can display logs from both the current, active log file and any compressed log files.

Types of logs collected for each device

FortiManager can collect logs from managed FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiSandbox, FortiWeb, FortiClient, and syslog servers. Following is a description of the types of logs FortiManager collects from each type of device:

Device Type	Log Type
FortiManager	Event
FortiAuthenticator	Event
FortiGate	Traffic Security: Antivirus, Intrusion Prevention, Application Control, Web Filter, DNS, Data Leak Prevention, Email Filter, Web Application Firewall, Vulnerability Scan, VoIP, FortiClient Event: Endpoint, HA, Compliance, System, Router, VPN, User, WAN Opt. & Cache, WiFi
FortiCarrier	Traffic, Event, GTP
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic, Event, Vulnerability Scan
FortiDDoS	Event, Intrusion Prevention
FortiMail	History, Event, Antivirus, Email Filter

Device Type	Log Type
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention, Traffic
Syslog	Generic

Traffic logs

Traffic logs record the traffic flowing through your FortiGate unit. Since traffic needs firewall policies to properly flow through FortiGate, this type of logging is also called firewall policy logging. Firewall policies control all traffic attempting to pass through the FortiGate unit, between FortiGate interfaces, zones, and VLAN sub-interfaces.

Security logs

Security logs (FortiGate) record all antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, vulnerability scan, and VoIP activity on your managed devices.

DNS logs

DNS logs (FortiGate) record the DNS activity on your managed devices.

Event logs

Event logs record administration management and Fortinet device system activity, such as when a configuration changes, or admin login or HA events occur. Event logs are important because they record Fortinet device system activity which provides valuable information about how your Fortinet unit is performing. FortiGate event logs includes *System*, *Router*, *VPN*, *User*, and *WiFi* menu objects to provide you with more granularity when viewing and searching log data.



The logs displayed on your FortiManager depends on the device type logging to it and the enabled features. FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox, FortiClient, and Syslog logging is supported. ADOMs must be enabled to support non-FortiGate logging.

For more information on logging see the *Logging and Reporting for FortiOS Handbook* in the [Fortinet Document Library](#).

Log messages

You can view log information by device or by log group.

Viewing the log message list of a specific log type

You can find FortiMail and FortiWeb logs in their default ADOMs.

To view the log message list:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type from the tree menu.
The corresponding log messages list is displayed.

Viewing log message details

To view log message details:

1. Double-click a log message on the log message list.

The log details pane is displayed to the right of the log message list, with the log fields categorized in tree view.



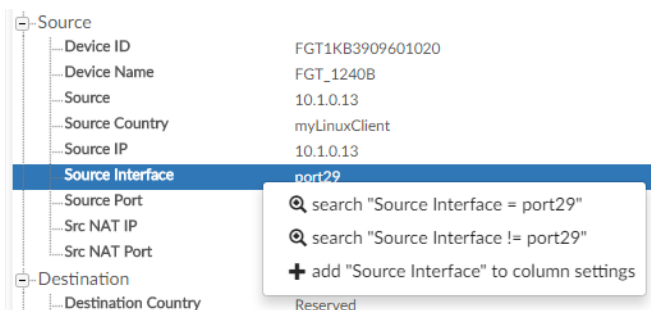
#	Date/Time	Device ID	Firewall Action	Source IP	User	Destination IP	Service	Application
1	14:12:50	FGT37D461580...	close	119.136.144.74		208.91.114.151	SMTPS	SMTPS
2	14:12:50	FGT37D461580...	close	172.16.181.178		172.16.181.178	4431/tcp	4431/tcp
3	14:12:50	FGT37D461580...	close	107.178.194.41		208.91.114.177	HTTP	HTTPBROWSER
4	14:12:50	FGT37D461580...	accept	172.16.100.80		151.80.195.199	DNS	DNS
5	14:12:50	FGT37D461580...	accept	172.16.100.80		192.48.79.30	DNS	DNS
6	14:12:50	FGT37D461580...	close	76.19.12.250		208.91.114.45	HTTP	HTTPBROWSER
7	14:12:50	FGT37D461580...	accept	165.21.100.94		208.91.114.22	DNS	DNS
8	14:12:50	FGT37D461580...	accept	172.16.100.80		34.224.202.237	DNS	DNS
9	14:12:50	FGT37D461580...	accept	172.16.100.80		192.43.172.30	DNS	DNS
10	14:12:50	FGT37D461580...	accept	74.125.113.133		208.91.114.22	DNS	DNS
11	14:12:50	FGT37D461580...	accept	172.16.69.132		172.16.100.100	DNS	DNS

The details pane on the right shows a tree view of log fields:

- Security
 - Level: notice
- General
 - Log ID: 13
 - Session ID: 2411535543
 - Time Stamp: 2018-03-13 14:12:50
 - Tran Display: dnst
 - Virtual Domain: root
- Source
 - Device ID: FGT37D4615801113
 - Device Name: Srv100
 - Source: 119.136.144.74
 - Source Country: China
 - Source IP: 119.136.144.74
 - Source Interface: INTERNET

You can display the log details pane below the log message list by clicking the *Bottom* icon in the log details pane. When the log details pane is displayed below the log message list, you can move it to the right of the log message list by clicking the *Right* icon. This is sometimes referred to as docking the pane to the bottom or right of the screen.

The log details pane provides shortcuts for adding filters and for showing or hiding a column. Right-click a log field to select an option.





If the log message contains UTM logs, you can click the UTM log icon in the log details pane to open the UTM log view window.

Customizing displayed columns

The columns displayed in the log message list can be customized and reordered as needed.

To customize what columns to display:

1. In the toolbar of the log message list view, click *Column Settings* and select a column to hide or display. The available columns vary depending on the device and log type.
2. To add other columns, click *More Columns*. In the *Column Settings* dialog box, select the columns to show or hide.
3. To reset to the default columns, click *Reset to Default*.
4. Click *OK*.



You can also add or remove a log field column in the log details pane, by right-clicking a log field and selecting *Add [log field name]* or *Remove [log field name]*.

To change the order of the displayed columns:




Place the cursor in the column title and move a column by drag and drop.

Filtering log messages

You can apply filters to the message list. Filters are not case-sensitive by default. If available, select *Tools > Case Sensitive Search* to create case-sensitive filters.



Filtering messages using filters in the toolbar

1. Go to the view you want.

Regular search	Click <i>Add Filter</i> and select a filter from the dropdown list, then type a value. Only displayed columns are available in the dropdown list. You can use search operators in regular search.
Switching between regular search and advanced search	At the right end of the <i>Add Filter</i> box, click the <i>Switch to Advanced Search</i> icon  or click the <i>Switch to Regular Search</i> icon  .
Advanced search	In Advanced Search mode, enter the search criteria (log field names and values).
Search operators and syntax	If available, click  at the right end of the <i>Add Filter</i> box to view search operators and syntax. See also Search operators and syntax on page 417 .
CLI string “freestyle” search	<p>Searches the string within the indexed fields configured using the CLI command: <code>config ts-index-field</code>.</p> <p>For example, if the indexed fields have been configured using these CLI commands:</p> <pre>config system sql config ts-index-field edit "FGT-traffic" set value "app,dstip,proto,service,srcip,user,utmaction" next end end</pre> <p>Then if you type “Skype” in the <i>Add Filter</i> box, FortiAnalyzer searches for “Skype” within these indexed fields: app,dstip,proto,service,srcip,user and utmaction.</p> <p>You can combine freestyle search with other search methods, for example: Skype user=David.</p>

2. In the toolbar, make other selections such as devices, time period, which columns to display, etc.

Filtering messages using the right-click menu

In a log message list, right-click an entry and select a filter criterion. The search criterion with a  icon returns entries matching the filter values, while the search criterion with a  icon returns entries that do not match the filter values.

Depending on the column in which your cursor is placed when you right-click, *Log View* uses the column value as the filter criteria. This context-sensitive filter is only available for certain columns.



To see log field name of a filter/column, right-click the column of a log entry and select a context-sensitive filter. The *Add Filter* box shows log field name.

Context-sensitive filters are available for each log field in the log details pane. See [Viewing log message details on page 414](#).

Filtering messages using smart action filters

For *Log View* windows that have an *Action* column, the *Action* column displays smart information according to policy (log field action) and utmaction (UTM profile action).

The *Action* column displays a green checkmark *Accept* icon when both policy and UTM profile allow the traffic to pass through, that is, both the log field action and UTM profile action specify *allow* to this traffic.

The *Action* column displays a red X *Deny* icon and the reason when either the log field action or UTM profile action deny the traffic.

If the traffic is denied due to policy, the deny reason is based on the policy log field action.

If the traffic is denied due to UTM profile, the deny reason is based on the FortiView *threattype* from *craction*. *craction* shows which type of threat triggered the UTM action. The *threattype*, *craction*, and *crscore* fields are configured in FortiGate in Log & Report. For more information, see the *FortiOS - Log Message Reference* in the *Fortinet Document Library*.

A filter applied to the *Action* column is always a smart action filter.



The smart action filter uses the FortiGate UTM profile to determine what the *Action* column displays. If the FortiGate UTM profile has set an action to *allow*, then the *Action* column will display that line with a green *Accept* icon, even if the *craction* field defines that traffic as a threat. The green *Accept* icon does not display any explanation.

In the scenario where the *craction* field defines the traffic as a threat but the FortiGate UTM profile has set an action to *allow*, that line in the Log View *Action* column displays a green *Accept* icon. The green *Accept* icon does not display any explanation.

Search operators and syntax

Operators or symbols	Syntax
And	Find log entries containing all the search terms. Connect the terms with a space character, or "and". Examples: <ol style="list-style-type: none"> 1. user=henry group=sales 2. user=henry and group=sales
Or	Find log entries containing any of the search terms. Separate the terms with "or" or a comma ",". Examples: <ol style="list-style-type: none"> 1. user=henry or srcip=10.1.0.15 2. user=henry,linda
Not	Find log entries that do NOT contain the search terms. Add "-" before the field name. Example: -user=henry
>, <	Find log entries greater than or less than a value, or within a range. This operator only applies to integer fields. Example: policyid>1 and policyid<10

Operators or symbols	Syntax
IP subnet/range search	Find log entries within a certain IP subnet or range. Examples: <ol style="list-style-type: none"> 1. <code>srcip=192.168.1.0/24</code> 2. <code>srcip=10.1.0.1-10.1.0.254</code>
Wildcard search	You can use wildcard searches for all field types. Examples: <ol style="list-style-type: none"> 1. <code>srcip=192.168.1.*</code> 2. <code>policyid=1*</code> 3. <code>user=*</code>

Filtering FortiClient log messages in FortiGate traffic logs

For FortiClient endpoints registered to FortiGate devices, you can filter log messages in FortiGate traffic log files that are triggered by FortiClient.

To Filter FortiClient log messages:

1. Go to *Log View > Traffic*.
2. In the *Add Filter* box, type `fct_devid=*`. A list of FortiGate traffic logs triggered by FortiClient is displayed.
3. In the message log list, select a FortiGate traffic log to view the details in the bottom pane.
4. Click the *FortiClient* tab, and double-click a FortiClient traffic log to see details.

The *FortiClient* tab is available only when the FortiGate traffic logs reference FortiClient traffic logs.

Viewing historical and real-time logs

By default, *Log View* displays historical logs. *Custom View* and *Chart Builder* are only available in historical log view.

To view real-time logs, in the log message list view toolbar, click *Tools > Real-time Log*.

To switch back to historical log view, click *Tools > Historical Log*.

Viewing raw and formatted logs

By default, *Log View* displays formatted logs. The log view you select affects available view options. You cannot customize columns when viewing raw logs.

To view raw logs, in the log message list view toolbar, click *Tools > Display Raw*.

To switch back to formatted log view, click *Tools > Formatted Log*.

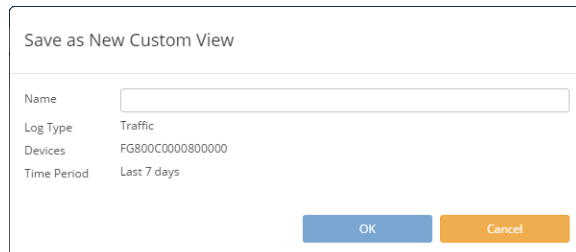
For more information about FortiGate raw logs, see the *FortiGate Log Message Reference* in the [Fortinet Document Library](#). For more information about raw logs of other devices, see the *Log Message Reference* for the platform type.

Custom views

Use *Custom View* to save the filter setting, device selection, and the time period you have specified.

To create a new custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the content pane, customize the log view as needed by adding filters, specifying devices, and/or specifying a time period.
4. In the toolbar, click *Custom View*.



5. In the *Name* field, type a name for the new custom view.
6. Click *OK*. The custom view is now displayed under *Log View > Custom View*.

To edit a custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Log View > Custom View*.
3. In the toolbar, edit the filter settings, and click *GO*.
4. In the toolbar, click *Custom View*.
5. Click *Save* to save the changes to the existing custom view or click *Save as* to save the changes to a new custom view.
6. Click *OK*.

To view the traffic log of a custom view:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Log View > Custom View*.
3. Right-click the name of a custom view and select *View Traffic*.

Downloading log messages

You can download historical log messages to the management computer as a text or CSV file. You cannot download real-time log messages.

To download log messages:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools > Download*.
4. In the *Download Logs* dialog box, configure download options:
 - In the *Log file format* dropdown list, select *Text* or *CSV*.
 - To compress the downloaded file, select *Compress with gzip*.

- To download only the current log message page, select *Current Page*. To download all the pages in the log message list, select *All Pages*.
5. Click *Download*.

Creating charts



You can also create charts in *Reports > Report Definitions > Chart Library*. See [Chart library on page 460](#)

Log View includes a *Chart Builder* for you to build custom charts for each type of log messages.

To create charts with Chart Builder:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools > Chart Builder*.
4. In the *Chart Builder* dialog box, configure the chart and click *Save*.

Name	Type a name for the chart.
Columns	Select which columns of data to include in the chart based on the log messages that are displayed on the <i>Log View</i> page.
Group By	Select how to group data in the chart.
Order By	Select how to order data in the chart.
Sort	Select a sort order for data in the chart.
Show Limit	Show Limit
Device	Displays the device(s) selected on the Log View page.
Time Frame	Displays the time frame selected on the Log View page.
Query	Displays the query being built.
Preview	Displays a preview of the chart.

Log groups

You can group devices into log groups. You can view FortiView summaries, display logs, generate reports, or create handlers for a log group. Log groups are virtual so they do not have SQL databases or occupy additional disk space.



In FortiManager 5.0.6 and earlier, you can treat log groups as a single device that has its own SQL database. You cannot do this in FortiManager 5.2 and later.

When you add a device with VDOMs to a log group, all VDOMs are automatically added.

To create a new log group:

1. Go to *Log View > Log Group*.
2. In the content pane toolbar, click *Create New*.
3. In the *Create New Log Group* dialog box, type a log group name and add devices to the log group.
4. Click *OK*.

Log browse

When a log file reaches its maximum size or a scheduled time, FortiManager rolls the active log file by renaming the file. The file name is in the form of `xlog.N.log`, where `x` is a letter indicating the log type, and `N` is a unique number corresponding to the time the first log entry was received. For information about setting the maximum file size and log rolling options, see [Device logs on page 522](#).

Log Browse displays log files stored for both devices and the FortiAnalyzer itself, and you can logs in the compressed phase of the log workflow.



In Collector mode, if you want to view the latest log messages, select the latest log file to display its log messages.

To view log files:

1. Go to *Log View > Log Browse*
2. Select a log file, and click *Display* to open the log file and display the log messages in formatted view.

You can perform all the same actions as with the log message list. See [Viewing log message details on page 414](#).

Display Delete Download Import Search...								
<input type="checkbox"/>	Device	Serial Number	VDOM	Type	Log Files	From	To	Size(bytes)
<input type="checkbox"/>	FG800C3912801080	FG800C3912801080	root	Event.	elog.log	Mon Oct 19 11:09:43 2015	Tue Nov 3 15:32:40 2015	3,013,855
<input type="checkbox"/>	FG800C3912801080	FG800C3912801080	root	Traffic.	tlog.log	Tue Nov 3 15:29:29 2015	Tue Nov 3 15:33:26 2015	29,034,845
<input type="checkbox"/>	FG800C3913802271	FG800C3913802271	root	Event.	elog.log	Thu Dec 10 16:14:29 2015	Mon Dec 14 15:08:36 2015	196,994,162
<input type="checkbox"/>	FG800C3913802271	FG800C3913802271	root	Traffic.	tlog.log	Mon Dec 14 11:11:49 2015	Mon Dec 14 15:08:36 2015	137,316,667
<input type="checkbox"/>	FGT37D4615800568	FGT37D4615800568	root	Event.	elog.log	Sun Dec 13 17:39:20 2015	Mon Dec 14 15:08:37 2015	121,906,049
<input type="checkbox"/>	FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.log	Mon Dec 14 15:06:51 2015	Mon Dec 14 15:08:37 2015	76,985,646
<input type="checkbox"/>	FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450134096.log.gz	Mon Dec 14 15:01:36 2015	Mon Dec 14 15:06:51 2015	35,530,685
<input type="checkbox"/>	FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450133752.log.gz	Mon Dec 14 14:55:52 2015	Mon Dec 14 15:01:36 2015	38,151,943
<input type="checkbox"/>	FGT37D4615800568	FGT37D4615800568	root	Traffic.	tlog.1450133466.log.gz	Mon Dec 14 14:51:06 2015	Mon Dec 14 14:55:52 2015	38,496,563

Importing a log file

Imported log files can be useful when restoring data or loading log data for temporary use. For example, if you have older log files from a device, you can import these logs to the FortiManager unit so that you can generate reports containing older data.

To insert imported logs into the SQL database, the `config system sqlstart-time` and `rebuild-event-start-time` must be **older** than the date of the logs that are imported **and** the storage policy for analytic data (the *Keep Logs for Analytics* field) must also extend back far enough.

To set the SQL start time and rebuild event start time using CLI commands:

```
config system sql
  set start-time <start-time-and-date>
  set rebuild-event-start-time <start-time-and-date>
end
```

Where `<start-time-and-date>` is in the format `hh:mm yyyy/mm/dd`.

To import a log file:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View > Log Browse* and click *Import* in the toolbar.
3. In the *Device* dropdown list, select the device the imported log file belongs to or select *[Take From Imported File]* to read the device ID from the log file.
If you select *[Take From Imported File]*, the log file must contain a `device_id` field in its log messages.
4. Drag and drop the log file onto the dialog box, or click *Add Files* and locate the file to be imported on your local computer.
5. Click *OK*. A message appears, stating that the upload is beginning, but will be canceled if you leave the page.
6. Click *OK*. The upload time varies depending on the size of the file and the speed of the connection.

After the log file is successfully uploaded, FortiManager inspects the file:

- If the `device_id` field in the uploaded log file does not match the device, the import fails. Click *Return* to try again.
- If you selected *[Take From Imported File]* and the FortiManager unit's device list does not currently contain that device, a message appears after the upload. Click *OK* to import the log file and automatically add the device to the device list.

Downloading a log file

You can download a log file to save it as a backup or to use outside the FortiManager unit. The download consists of either the entire log file, or a partial log file, as selected by your current log view filter settings and, if downloading a raw file, the time span specified.

To download a log file:

1. Go to *Log View > Log Browse* and select the log file that you want to download.
2. In the toolbar, click *Download*.

3. In the *Download Log File(s)* dialog box, configure download options:
 - In the *Log file format* dropdown list, select *Native*, *Text*, or *CSV*.
 - If you want to compress the downloaded file, select *Compress with gzip*.
4. Click *Download*.

Deleting log files

To delete log files:

1. Go to *Log View > Log Browse*.
2. Select one or more files and click *Delete*.
3. Click *OK* to confirm.

Event Management

Event Management displays all events generated by event handlers.

How ADOMs affect events

When ADOMs are enabled, each ADOM has its own event handlers and lists of events. Ensure you are in the correct ADOM before viewing *Event Management*. See [Switching between ADOMs on page 37](#).

Predefined event handlers

You can use predefined event handlers to generate events for *Event Management*. There are predefined event handlers for FortiGate and FortiCarrier devices. For other devices, you can create custom event handlers.

Logs used for events

Event Management displays events from Analytics logs, not Archive logs.



This pane is only available when the FortiAnalyzer features are enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Event handlers

Event handlers define what messages to extract from logs and display in Event Management. You must enable an event handler to start generating events. To see which event handlers are enabled or disabled, see [Enabling event handlers on page 432](#).

You can configure event handlers to generate events for a specific device, for all devices, or for the local FortiManager unit. You can create event handlers for FortiGate, FortiCarrier, FortiCache, FortiMail, FortiManager, FortiWeb, FortiSandbox devices, and syslog servers. In 5.2.0 or later, Event Management supports local FortiManager event logs.

You can configure the system to send you alerts for event handlers. You can send the alert to an email address, SNMP community, or syslog server.

Managing event handlers

To manage event handlers, go to *Event Management > Event Handler List*. The following options are available:

Option	Description
Create New	Create a new event handler.
Edit	Edit the selected event handler.
Delete	Delete the selected event handler. You cannot delete predefined event handlers.
Clone	Clone the selected event handler.
Enable	Enable the selected event handler to start generating events on the <i>Event Management > All Events</i> page.
Disable	Disable the selected event handler to stop generating events on the <i>Event Management > All Events</i> page.
Collapse All / Expand All	Collapse or expand the <i>Filters</i> column.
Show Predefined	Show or hide predefined handlers in the list.
Show Custom	Show or hide custom handlers in the list.
Factory Reset	If you have modified a predefined event handler, return the selected predefined event handler to its factory default settings.

List of predefined event handlers

FortiManager includes predefined event handlers for FortiGate and FortiCarrier devices that you can use to generate events.

Event Handler	Description
Antivirus Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Traffic Event Category: Antivirus Group by: Virus Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Level Greater Than or Equal To Information</i> Generic Text Filter: <code>virus!=''</code> and <code>virus!='N/A'</code>

Event Handler	Description
App Ctrl Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Critical Log Type: Traffic Event Category: Application Control Group by: Application Name Log messages that match any of the following conditions: <ul style="list-style-type: none"> <i>Application Category Equal To Botnet</i> <i>Application Category Equal To Proxy</i>
Application Crashed Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Event Log Event Category: System Group by: Log Description Log messages that match all conditions: <ul style="list-style-type: none"> <i>Log Description Equal To Application crashed</i> <i>Level Greater Than or Equal To Warning</i>
Botnet Application Allowed by Application Control	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Critical Log Type: Application Control Group by: Application Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Application Category Equal to Botnet</i> <i>(action==pass or action==monitor)</i>
Botnet Application Blocked by Application Control	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: High Log Type: Application Control Group by: Application Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Application Category Equal to Botnet</i> <i>Action Not Equal to Pass</i> <i>Action Not Equal to Monitor</i>
Botnet C-and-C Allowed by IP-Reputation	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: High Log Type: Application Control Group by: Virus Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Action Not Equal to Blocked</i> <i>logid==0202009248 or logid==0202009249</i>

Event Handler	Description
Botnet C-and-C Blocked by DNS Filtering	Disabled by default <ul style="list-style-type: none"> Severity: Medium Log Type: DNS Group by: Message Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Level Greater Than or Equal to Information</i> <i>logid==1501054600 or logid==1501054601</i>
Botnet C-and-C Blocked by IP-Reputation	Disabled by default <ul style="list-style-type: none"> Severity: Medium Log Type: AntiVirus Group by: Virus Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Action Equal to Blocked</i> <i>logid==0202009248 or logid==0202009249</i>
Botnet Traffic Allowed by IPS	Disabled by default <ul style="list-style-type: none"> Severity: Critical Log Type: IPS Group by: Attack Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Level Greater Than or Equal To Information</i> <i>attack ~ Botnet and (action=='detected' or action=='pass session')</i>
Botnet Traffic Blocked by IPS	Disabled by default <ul style="list-style-type: none"> Severity: High Log Type: IPS Group by: Attack Name Log messages that match all of the following conditions: <ul style="list-style-type: none"> <i>Level Greater Than or Equal To Information</i> <i>attack ~ Botnet and (action!='detected' or action!='pass session')</i>
Conserve Mode	Disabled by default <ul style="list-style-type: none"> Severity: Critical Log Type: Event Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <i>Log Description Equal To System services entered conserve mode</i>

Event Handler	Description
DLP Event	Disabled by default <ul style="list-style-type: none"> Severity: Medium Log Type: Traffic Log Event Category: DLP Group by: DLP Rule Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Security Action Equal To Blocked</i>
DNS Botnet C-and-C - High Severity	Enabled by default <ul style="list-style-type: none"> Severity: High Log Type: DNS Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <i>Level Equal To Warning</i> Generic Text Filter: <code>botnetip!='' or botnetdomain!=''</code>
HA Failover	Disabled by default <ul style="list-style-type: none"> Severity: Medium Log Type: Event Log Event Category: HA Group by: Log Description Log messages that match any of the following conditions: <ul style="list-style-type: none"> <i>Log Description Equal To Virtual cluster move member</i> <i>Log Description Equal To Virtual cluster member state moved</i>
Interface Down	Disabled by default <ul style="list-style-type: none"> Severity: High Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To interface-stat-change</i> <i>Status Equal To DOWN</i>
Interface Up	Disabled by default <ul style="list-style-type: none"> Severity: Medium Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To interface-stat-change</i> <i>Status Equal To UP</i>



Event Handler	Description
IPS - Critical Severity	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Critical Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Severity Equal To Critical</i>
IPS - High Severity	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: High Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Severity Equal To High</i>
IPS - Low Severity	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Low Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Severity Equal To Low</i>
IPS - Medium Severity	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: IPS Group by: Attack Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Severity Equal To Medium</i>
IPsec Phase2 Down	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Event Log Event Category: VPN Group By: VPN Tunnel Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To phase2-down</i>
IPsec Phase2 Up	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Event Log Event Category: VPN Group By: VPN Tunnel Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To phase2-up</i>

Event Handler	Description
Local Device Event	<p>Found only in the Root ADOM.</p> <p>Enabled by default</p> <ul style="list-style-type: none"> • Devices: Local Device • Severity: Medium • Log Type: Event Log • Event Type: Any • Group By: Device ID • Log messages that match any of the following conditions: <ul style="list-style-type: none"> • <i>Level Equal To Emergency</i>
Malware Traffic Allowed By AntiVirus	<p>Disabled by default</p> <ul style="list-style-type: none"> • Severity: High • Log Type: AntiVirus • Group By: Virus Name • Log messages that match all conditions: <ul style="list-style-type: none"> • <i>Level Greater Than or Equal to Information</i> • <i>logid==0211008193 or logid==0211008195</i>
Malware Traffic Allowed by FortiSandbox	<p>Disabled by default</p> <ul style="list-style-type: none"> • Severity: High • Log Type: AntiVirus • Group By: Virus Name • Log messages that match all conditions: <ul style="list-style-type: none"> • <i>Level Greater Than or Equal to Information</i> • <i>logid==0211009235 or logid==0211009237</i>
Malware Traffic Blocked by AntiVirus	<p>Disabled by default</p> <ul style="list-style-type: none"> • Severity: Medium • Log Type: AntiVirus • Group By: Virus Name • Log messages that match all conditions: <ul style="list-style-type: none"> • <i>Level Greater Than or Equal to Information</i> • <i>logid==0211008192 or logid==0211008194</i>
Malware Traffic Blocked by FortiSandbox Signature Update	<p>Disabled by default</p> <ul style="list-style-type: none"> • Severity: Medium • Log Type: AntiVirus • Group By: Virus Name • Log messages that match all conditions: <ul style="list-style-type: none"> • <i>Level Greater Than or Equal to Information</i> • <i>logid==0211009234 or logid==0211009236</i>

Event Handler	Description
Power Supply Failure	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Critical Log Type: Event Log Event Category: System Group by: Message Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To power-supply-monitor</i> <i>Status Equal To failure</i>
UTM Antivirus Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: High Log Type: Antivirus Log Group by: Virus Name Log messages that match all conditions: <ul style="list-style-type: none"> <i>Level Greater Than or Equal To Information</i> Generic Text Filter: <code>virus!=''</code> and <code>virus!='N/A'</code> and <code>dtype!='fortisandbox'</code>
UTM App Ctrl Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Critical Log Type: Application Control Group by: Application Name Log messages that match any of the following conditions: <ul style="list-style-type: none"> <i>Application Category Equal To Botnet</i> <i>Application Category Equal To Proxy</i>
UTM DLP Event	<p>Disabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: DLP Group by: Profile Log messages that match all conditions: <ul style="list-style-type: none"> <i>Action Equal To Block</i>

Event Handler	Description
UTM Web Filter Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Web Filter Group by: Category Log messages that match any of the following conditions: <ul style="list-style-type: none"> <i>Web Category Equal To Child Abuse</i> <i>Web Category Equal To Discrimination</i> <i>Web Category Equal To Drug Abuse</i> <i>Web Category Equal To Explicit Violence</i> <i>Web Category Equal To Extremist Groups</i> <i>Web Category Equal To Hacking</i> <i>Web Category Equal To Illegal or Unethical</i> <i>Web Category Equal To Plagiarism</i> <i>Web Category Equal To Proxy Avoidance</i> <i>Web Category Equal To Malicious Websites</i> <i>Web Category Equal To Phishing</i> <i>Web Category Equal To Spam URLs</i>
Web Filter Event	<p>Enabled by default</p> <ul style="list-style-type: none"> Severity: Medium Log Type: Traffic Log Event Category: Web Filter Group by: Category Log messages that match any of the following conditions: <ul style="list-style-type: none"> <i>Web Category Equal To Child Abuse</i> <i>Web Category Equal To Discrimination</i> <i>Web Category Equal To Drug Abuse</i> <i>Web Category Equal To Explicit Violence</i> <i>Web Category Equal To Extremist Groups</i> <i>Web Category Equal To Hacking</i> <i>Web Category Equal To Illegal or Unethical</i> <i>Web Category Equal To Plagiarism</i> <i>Web Category Equal To Proxy Avoidance</i> <i>Web Category Equal To Malicious Websites</i> <i>Web Category Equal To Phishing</i> <i>Web Category Equal To Spam URLs</i>

Enabling event handlers

For both predefined and custom event handlers, you must enable the event handler to generate events. In the *Event Handler List*, the *Name* column displays a  icon for enabled event handlers and a  icon for disabled event

handlers.

If you want to receive alerts for predefined events handlers, edit the predefined event handler to configure notifications.

To enable event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management > Event Handler List*.
3. Select one or more event handlers and click *More > Enable* or right-click an event handler and select *Enable*.

Creating custom event handlers

To create a new event handler:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management > Event Handler List*.
3. In the toolbar, click *Create New*.

Create New Handler

Status: ☒ ON

Name:

Description:

Devices: ☒ All Devices ☐ Specify ☐ Local Device

Severity:

Filters

Log Type:

Event Category:

Group By:

Logs match: ☐ All ☒ Any of the following conditions

Log Field	Match Criteria	Value
<input type="text" value="Level"/>	<input type="text" value="Equal To"/>	<input type="text" value="Emergency"/>

Generic Text Filter:

Notifications

Generate alert when at least matches occurred over a period of minutes

☐ Send Alert Email

☐ Send SNMP(v1/v2) Trap

☐ Send SNMP(v3) Trap

☐ Send Alert to Syslog Server

☐ Send Each Alert Separately

OK Cancel

4. Configure the settings as required and click **OK**. For a description of the fields, see [Create New Handler pane on page 434](#).
5. Click **OK** to create the new event handler.

Creating custom event handlers using the Generic Text Filter

The *Generic Text Filter* uses regex (regular expression) syntax. You must use an escape character when needed. For example, `cfgpath=firewall.policy` is the wrong syntax because it's missing an escape character. The correct syntax is `cfgpath=firewall\.policy`.

To create an event handler using the Generic Text Filter to match raw log data:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Log View*, and select a log type.
3. In the toolbar, click *Tools > Display Raw*.
The easiest method is to copy the text string you want from the raw log and paste it into the *Generic Text Filter* field. Ensure you insert an escape character when necessary, for example, `cfgpath=firewall\.policy`.
4. Locate and copy the text in the raw log.
5. Go to *Event Management > Event Handler List* and click *Create New*.
6. In the *Generic Text Filter* box, paste the text you copied or type the text you want. Ensure you use the raw log field names, for example, `mem` (not memory) and `setuprate` (not setup-rate).
For information on text format and operators, hover the cursor over the help icon. The operator `~` means contains and `!~` means does not contain.
7. If you want to be notified of events, configure the *Notifications* section.
8. Configure other settings as required and click *OK*. For a description of the fields, see [Create New Handler pane on page 434](#).

Create New Handler pane

Following is a description of the options available in the *Create New Handler* pane:

Field	Description
Status	Enable or disable the event handler.
Name	Add a name for the handler.
Description	Type a description of the event handler.
Devices	Select the devices to include. <ul style="list-style-type: none"> • <i>All Devices</i>. • <i>Specify</i>: To add devices, click the Add icon. • <i>Local Device</i>: Select if the event handler is for local FortiManager event logs. This option is only available in the root ADOM and is used to query FortiManager event logs. For <i>Local Device</i>, the <i>Log Type</i> must be <i>Event Log</i> and <i>Event Category</i> must be <i>Any</i>.
Severity	Select the severity from the dropdown list: <i>Critical</i> , <i>High</i> , <i>Medium</i> , or <i>Low</i> .
Filters	Configure filters for the handler.

Field	Description
Log Type	Select the log type from the dropdown list. When <i>Devices</i> is set to <i>Local Device</i> , you cannot change the <i>Log Type</i> or <i>Event Category</i> .
Event Category	Select the category of event that this handler monitors. The available options depends on the platform type. This option is only available when <i>Log Type</i> is set to <i>Event Log</i> or <i>Traffic Log</i> .
Group By	Select how to group the events.
Logs match	Select <i>All</i> or <i>Any of the following conditions</i> .
Log Field	Select a log field to filter from the dropdown list. The available options depends on the selected log type.
Match Criteria	Select a match criteria from the dropdown list. The available options depends on the selected log field.
Value	Either select a value from the dropdown list or enter a value in the text box. The available options depends on the selected log field.
Add	Add log filter. When <i>Devices</i> is set to <i>Local Device</i> this option is not available. You can only have one log field filter.
Remove	Delete the filter.
Generic Text Filter	Enter a generic text filter. For more information on creating a generic text filter, see Creating custom event handlers using the Generic Text Filter on page 434 . For information on text format, hover the cursor over the help icon. The operator ~ means contains and ! ~ means does not contain.
Notifications	Configure alerts for the handler.
Generate alert when at least <i>n</i> matches occurred over a period of <i>n</i> minutes	Enter threshold values to generate alerts. Enter the number of matching events that must occur in the number of minutes to generate an alert.
Send Alert Email	Send an alert by email. Specify email parameters including the mail server. For more information, see Mail Server on page 518 .
Send SNMP(...) Trap	Select one or both checkboxes and specify an SNMP community or user from the dropdown list. Click the add icon to create a new SNMP community or user. For more information, see SNMP on page 509 .
Send Alert to Syslog Server	Send an alert to the syslog server. Select a syslog server from the dropdown list. Click the add icon to create a new syslog server. For more information, see Syslog Server on page 520 .

Field	Description
Send Each Alert Separately	Select to send each alert individually instead of in a group.

Filtering event handlers

You can filter the list of event handlers to show only predefined or custom handlers.

To filter event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management > Event Handler List*.
3. In the toolbar, click *More > Show Predefined* or *More > Show Custom* to filter the event handlers.

Searching event handlers

To search event handlers:

1. Go to *Event Management > Event Handler List*.
2. Type a search term in the search box at the top-right.

Resetting to factory defaults

You can change predefined event handlers as needed. If required, you can restore predefined event handlers to factory default settings.

To reset predefined event handlers:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Event Management > Event Handler*.
3. Ensure the *Show Predefined* checkbox is selected.
4. Select one or more predefined event handlers.
5. Click *More > Factory Reset* to return the settings to factory defaults.



You can also reset predefined event handlers to factory default settings in the *Edit Handler* page.

Events

After event handlers start generating events, you can view events and event details. *Event Management > All Events* shows events by type and severity in a graphical format, and recent events in a tabular format. *Event Management > Calendar View* shows events by month or week in a calendar or bar chart format.

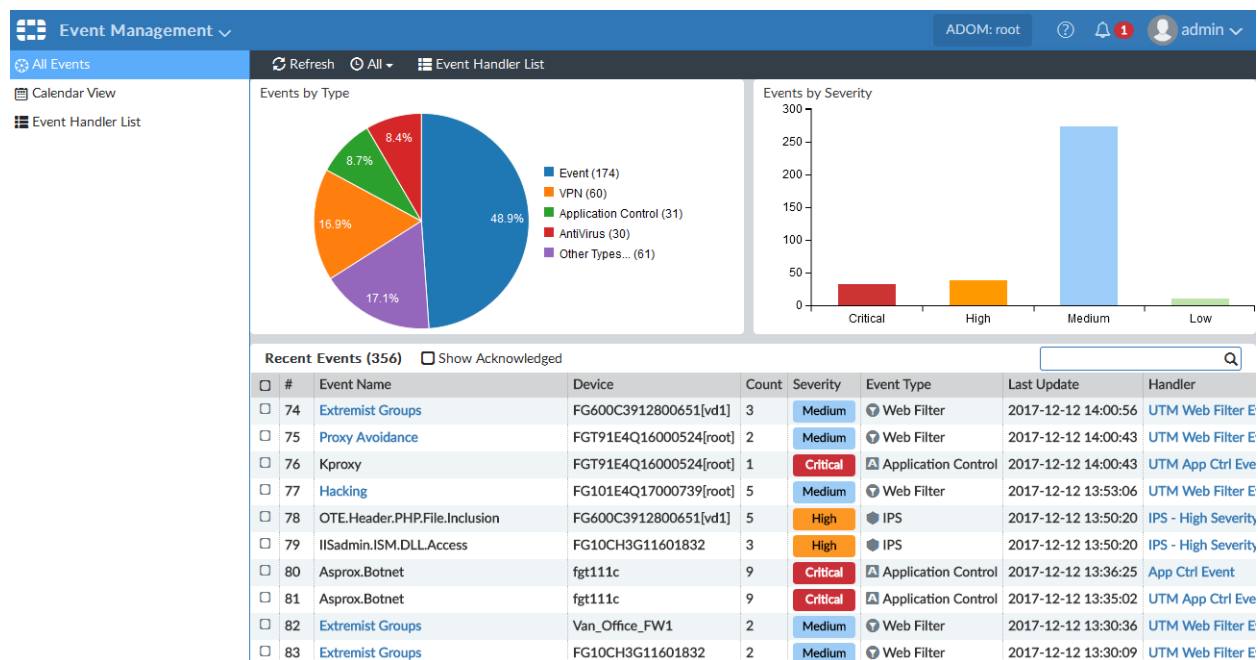


When rebuilding the SQL database, you might not see a complete list of historical events. However, you can always see events in real-time logs. You can view the status of the SQL rebuild by checking the *Rebuilding DB* status in the *Notification Center*.

Event summaries

- To view event summaries, go to *Event Management > All Events*.
- To manually refresh the event summaries data, click *Refresh*.
You can automatically set the refresh interval to *Every 10 Seconds*, *Every 30 Seconds*, *Every 1 Minute*, or *Every 5 Minutes*.
- To change the time period to display, click the time icon and specify a time period.
- To view event handlers, click *Event Handler List* (see [Event handlers on page 424](#)).

All Events show events by type and severity in a graphical format, and recent events in a tabular format.



Events by Type

Events by Type shows a pie chart organized by event type.

- To view the number of alerts (*Events*) and the number of logs (*Counts*) for that event type, hover the cursor over parts of the pie or legend.
- To view a list showing only that type of event, click on that element in the chart.

Events by Severity

Events by Severity shows a bar chart organized by event severity.

- To view the number of alerts (*Events*) and the number of logs (*Counts*) for that event severity, hover the cursor over a bar.
- To view a list showing only events with that severity, click on a bar in the chart.

Recent Events

Recent Events shows events for the selected time span.

- To sort by a column, click the column header.
- To include acknowledged events, click *Show Acknowledged*. See [Acknowledging events](#).
- To search the list, type a search term in the search box.
- To edit a handler, click a *Handler* element. See [Event handlers](#).
- To view information about an event and recommended actions, click its *Event Name* hyperlink. This option is only available for some events.
- To view event details, double-click the event line. See [Event details](#).

Filtered event list

In *Events by Type* and *Events by Severity*, click an element to show only events of that type or severity. The filtered event list shows the same information and options as the *Recent Events* list.

To return to the previous page, click the back button.

Event details

In *Recent Events* or a filtered events list, to view event details, double-click the event line or right-click the event and select *View Details*.

The screenshot displays the FortiManager Event Management interface. On the left, a sidebar shows event details for a 'Proxy:HTTP' event, including severity (Critical), type (Application Control), count (26), last update (2016-10-03 18:00:18), device (FGT37D0000800007), event handler (UTM App Ctrl Event), and a comment field. The main area shows a table of logs with columns: #, Date/Time, Level, Device ID, Group, Profile, Destination Port, and Source. The table lists 22 logs, all with 'Information' level. On the right, a 'Details' pane shows expanded information for the selected log, including Security Level (low), Threat Score (5), General Log ID (1010101010), Message (Proxy: Proxy:HTTP), Session ID (1000000000), Time Stamp (2016-00-03 18:23:55), Virtual Domain (root), Source, Destination, Action (pass), Policy ID (99), Application, Threat, Type, Event Type (app-ctrl-all), Sub Type (app-ctrl), and Type (utm). At the bottom, there are buttons for 'Save Comment', 'Acknowledge', and 'Hide Details', along with a status bar showing 'Total logs stored for analytics: 15 days 4 hours' and '1000 Items per page'.

The event details page contains information about the event and a list of all individual logs. You can print, acknowledge, and add comments to the event.

- To change what columns to display, click *Column Settings* or *Column Settings > More Columns*.
- To display more details, double-click a line or select a line and click *Display Details* in the bottom-right. The log details pane open on the right side of the window.
- To return to the previous page, click the back button.

Acknowledging events

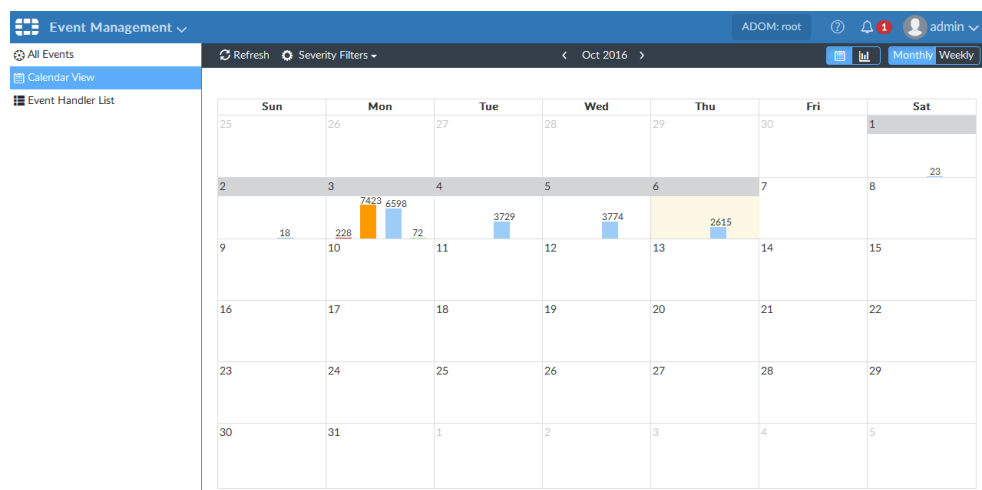
Acknowledging an event removes it from the recent events list (if *Show Acknowledged* is not selected).

To acknowledge events:

- In the recent events list, select one or more events, then right-click and select *Acknowledge*.
- In the event details page, click *Acknowledge*.

Event calendar

Calendar View shows events by month or week in a calendar or bar chart format.

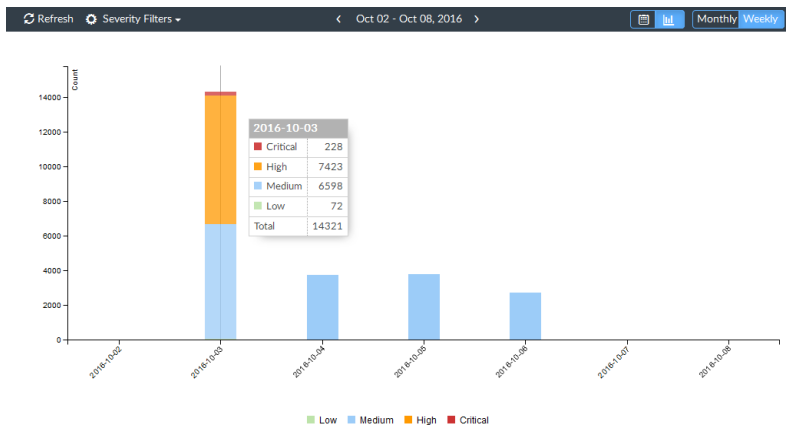


To include only events of a specific severity, click *Severity Filters* and select which severity levels to include. The default filter is critical and high severity.

Click on any element in any of the views to open the filtered events list; see [Filtered event list on page 438](#).

Click the *Calendar Chart* button in the toolbar to display the calendar. The monthly view of the calendar shows bar charts of the events by severity on each day of the month. The weekly view shows the events for each hour of each day of the week. Click the arrows on either side of the calendar heading to scroll through months or weeks.

Click the *Bar Chart* button in the toolbar to change to the bar chart view. The bar chart view shows a stacked, vertical bar chart of the count versus time (days). Hovering the cursor over a bar shows the number of logs of each severity and the total for that day.



Reports

You can generate data reports from logs by using the *Reports* feature. You can do the following:

- Use predefined reports. Predefined report templates, charts, and macros are available to help you create new reports.
- Create customize reports.

Report files are stored in the reserved space for the FortiManager device. See [Automatic deletion on page 207](#).



When rebuilding the SQL database, *Reports* are not available until the rebuild is completed. Select the *Show Progress* link in the message to view the status of the SQL rebuild.



This pane is only available when the FortiAnalyzer features are enabled. For more information, see [FortiAnalyzer Features on page 390](#).

How ADOMs affect reports

When ADOMs are enabled, each ADOM has its own reports, libraries, and advanced settings. Make sure you are in the correct ADOM before selecting a report. See [Switching between ADOMs on page 37](#).

Some reports are available only when ADOMs are enabled. For example, ADOMs must be enabled to access FortiCarrier, FortiCache, FortiClient, FortiDDoS, FortiMail, FortiSandbox, and FortiWeb reports. You can configure and generate reports for these devices within their respective default ADOM. These devices also have device-specific charts and datasets.

Predefined reports, templates, charts, and macros

FortiManager includes a number of predefined elements you can use to create and/or build reports.

Predefined...	GUI Location	Purpose
Reports	<i>Reports > Report Definitions > All Reports</i>	You can generate reports directly or with minimum setting configurations. Predefined reports are actually report templates with basic default setting configurations.
Templates	<i>Reports > Report Definitions > Templates</i>	You can use directly or build upon. Report templates include charts and/or macros and specify the layout of the report. A template populates the <i>Layout</i> tab of a report that is to be created. See List of report templates on page 458 .

Predefined...	GUI Location	Purpose
Charts	<i>Reports > Report Definitions > Chart Library</i>	You can use directly or build upon a report template you are creating, or in the <i>Layout</i> tab of a report that you are creating. Charts specify what data to extract from logs.
Macros	<i>Reports > Report Definitions > Macro Library</i>	You can use directly or build upon a report template that you are creating, or in the <i>Layout</i> tab of a report that you are creating. Macros specify what data to extract from logs.

Logs used for reports

Reports uses Analytics logs to generate reports. Archive logs are not used to generate reports.

For reports about users, the FortiGate needs to populate the `user` field in the logs sent to FortiAnalyzer. For more information see the *FortiOS Handbook > Authentication > Configuring authenticated access and Agent-based FSSO*.

How charts and macros extract data from logs

Reports include charts and/or macros. Each chart and macro is associated with a dataset. When you generate a report, the dataset associated with each chart and macro extracts data from the logs and populates the charts and macros. Each chart requires a specific log type.

FortiManager includes a number of predefined charts and macros. You can also create custom charts and macros.

How auto-cache works

When you generate a report, it can take days to assemble the required dataset and produce the report, depending on the required datasets. Instead of assembling datasets at the time of report generation, you can enable the *auto-cache* feature for the report.

Auto-cache is a setting that tells the system to automatically generate *hcache*. The *hcache* (hard cache) means that the cache stays on disk in the form of database tables instead of memory. *Hcache* is applied to “matured” database tables. When a database table rolls, it becomes “mature”, meaning the table will not grow anymore. Therefore, it is unnecessary to query this database table each time for the same SQL query, so *hcache* is used. *Hcache* runs queries on matured database tables in advance and caches the interim results of each query. When it is time to generate the report, much of the datasets are already assembled, and the system only needs to merge the results from *hcaches*. This reduces report generation time significantly.

The *auto-cache* process uses system resources to assemble and cache the datasets and it takes extra space to save the query results. You should only enable *auto-cache* for reports that require a long time to assemble datasets.

Generating reports

You can generate reports by using one of the predefined reports or by using a custom report that you created. You can find all the predefined reports and custom reports listed in *Reports > Report Definitions > All Reports*.

To generate a report:

1. Go to *Reports > Report Definitions > All Reports*.
2. In the content pane, select a report from the list.
3. (Optional) Click *Edit* in the toolbar and edit settings on the *Settings* and *Layout* tabs. For a description of the fields in the *Settings* and *Layout* tabs, see [Reports Settings tab on page 447](#) and [Creating charts on page 460](#) and [Macro library on page 463](#).
4. In the toolbar, click *Run Report*.

Viewing completed reports

After you generate reports, you can view completed reports in *Reports > Generated Reports* or *Reports > Report Definitions > All Reports*. You can view reports in the following formats: HTML, PDF, XML, and CSV.

To view completed reports in Generated Reports:

1. Go to *Reports > Generated Reports*.
This view shows all generated reports for the specified time period.
2. To sort the report list by date, click *Order by Time*. To sort the report list by report name, click *Order by Name*.
3. Locate the report and click the format in which you want to view the report to open the report in that format.
For example, if you want to review the report in HTML format, click the *HTML* link.

To view completed reports in All Reports:

1. Go to *Reports > Report Definitions > All Reports*.
2. On the report list, double-click a report to open it.
3. In the *View Report* tab, locate the report and click the format in which you want to view the report to open the report in that format.
For example, if you want to review the report in HTML format, click the *HTML* link.

Enabling auto-cache

You can enable auto-cache to reduce report generation time for reports that require a long time to assemble datasets. For information about auto-cache and hcache, see [How auto-cache works on page 442](#).

You can see the status of building the cache in *Reports > Report Definitions > All Reports* in the *Cache Status* column.

To enable auto-cache:

1. Go to *Reports > Report Definitions > All Reports*.
2. Select the report from the list, and click *Edit* in the toolbar.
3. In the *Settings* tab, select the *Enable Auto-cache* checkbox.
4. Click *Apply*.

Grouping reports

If you are running a large number of reports which are very similar, you can significantly improve report generation time by grouping the reports. Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-hcache* completion time.
- Improve report completion time.

Step 1: Configure report grouping

For example, to group reports with titles containing string `Security_Report` by device ID and VDOM, enter the following CLI commands:

```
config system report group
  edit 0
    set adom root
    config group-by
      edit devid
      next
      edit vd
      next
    end
    set report-like Security_Report
  next
end
```

Notes:

- The `report-like` field specifies the string in report titles that is used for report grouping. This string is case-sensitive.
- The `group-by` value controls how cache tables are grouped.
- To view report grouping information, enter the following CLI command, then check the Report Group column of the table that is displayed.
`execute sql-report list-schedule <ADOM>`

Step 2: Initiate a rebuild of hcache tables

To initiate a rebuild of hcache tables, enter the following CLI command:

```
diagnose sql hcache rebuild-report <start-time> <end-time>
```

Where `<start-time>` and `<end-time>` are in the format: `<yyyy-mm-dd hh:mm:ss>`.

Retrieving report diagnostic logs

Once you start to run a report, FortiAnalyzer creates a log about the report generation status and system performance. Use this diagnostic log to troubleshoot report performance issues. For example, if your report is very slow to generate, you can use this log to check system performance and see which charts take the longest time to generate.

For information on how to interpret the report diagnostic log and troubleshoot report performance issues, see the *FortiAnalyzer Report Performance Troubleshooting Guide*.

To retrieve report generation logs:

1. In *Reports > Generated Report*, right-click the report and select *Retrieve Diagnostic* to download the log to your computer.
2. Use a text editor to open the log.

Auto-Generated Reports

The *Cyber Threat Assessment* report is automatically generated. By default, the report will run at 3:00AM every Monday. For more information on report scheduling, see [Scheduling reports on page 445](#).

Schedules can be viewed in the *Report Calendar*. See "Report calendar" on page 471.



This will only affect newly installed FortiAnalyzer or newly created ADOM. Upgraded ADOM reports, scheduling and calendar will be kept as is.

Scheduling reports

You can configure a report to generate on a regular schedule. Schedules can be viewed in the *Report Calendar*. See [Report calendar on page 471](#).

To schedule a report:

1. Go to *Reports > Report Definitions > All Reports*.
2. Select a report and click *Edit* in the toolbar.
3. Click *Settings* in the toolbar.
4. Select the *Enable Schedule* checkbox and configure the schedule.
5. Click *Apply*.

Creating reports

You can create reports from report templates, by cloning and editing predefined/existing reports, or start from scratch.

Creating reports from report templates

You can create a new report from a template. The template populates the *Layout* tab of the report. The template specifies what text, charts, and macros to use in the report and the layout of the content. Report templates do not contain any data. Data is added to the report when you generate the report.

To create a new report from a template:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the toolbar, click *Create New*. The *Create Report* dialog box opens.

4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % \$ +
5. Select *From Template* for the *Create from* setting, then select a template from the dropdown list. The template populates the *Layout* tab of the report.
6. Select the folder that the new report will be saved to from the dropdown list. See [Organizing reports into folders on page 455](#) for information about folders.
7. Select *OK* to create the new report.
8. On the *Settings* tab, configure the settings as required. For a description of the fields, see [Reports Settings tab on page 447](#).
9. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see [Reports Layout tab on page 450](#).
10. Click *Apply* to save your changes.

Creating reports by cloning and editing

You can create reports by cloning and editing predefined and/or existing reports.

To create a report by cloning and editing:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, then click *Clone* in the toolbar.
4. In the *Clone Report* dialog box, type a name for the cloned report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % \$ +
5. Select the folder that the new report will be saved to from the dropdown list. See [Organizing reports into folders on page 455](#) for information about folders.
6. Select *OK* to create the new report.
7. On the *Settings* tab, configure the settings as required. For a description of the fields, see [Reports Settings tab on page 447](#).
8. Optionally, go to the *Layout* tab to customize the report layout and content. For a description of the fields, see [Reports Layout tab on page 450](#).
9. Click *Apply* to save your changes.

Creating reports without using a template

To create a report without using a template:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the toolbar, click *Create New*. The *Create New Report* dialog box opens.
4. In the *Name* box, type a name for the new report. The following characters are NOT supported in report names: \ / " ' < > & , | # ? % \$ +
5. Select the *Blank* option for the *Create from* setting.
6. Select the folder that the new report will be saved to from the dropdown list. See [Organizing reports into folders on page 455](#) for information about folders.
7. Select *OK* to create the new report.
8. On the *Settings* tab, you can specify a time period for the report, what device logs to include in the report, and so on. You can also add filters to the report, add a cover page to the report, and so on. For a description of the fields, see [Reports Settings tab on page 447](#).



To create a custom cover page, you must select *Print Cover Page* in the *Advanced Settings* menu.

9. On the *Layout* tab, you can specify the charts and macros to include in the report, as well as report content and layout.
For a description of the fields, see [Reports Layout tab on page 450](#).
For information about creating charts and macros, see [Creating charts on page 460](#) and [Creating macros on page 463](#).
10. Click *Apply* to save your changes.

Reports Settings tab

The following options are available in the *Settings* tab:

Field	Description
Time Period	The time period the report covers. Select a time period or select <i>Custom</i> to manually specify the start and end date and time.
Devices	The devices to include in the report. Select either <i>All Devices</i> or <i>Specify</i> to add specific devices. Select the add icon to select devices.
Type	Select either <i>Single Report (Group Report)</i> or <i>Multiple Reports (Per-Device)</i> . This option is only available if multiple devices are selected.
Enable Schedule	Select to enable report template schedules.

Field	Description
Enable Auto-Cache	Select to assemble datasets before generating the report and as the data is available. This process uses system resources and is recommended only for reports that require days to assemble datasets. Disable this option for unused reports and for reports that require little time to assemble datasets.
Generate PDF Report Every	Select when the report is generated. Enter a number for the frequency of the report based on the time period selected from the dropdown list.
Start time	Enter a starting date and time for the file generation.
End time	Enter an ending date and time for the file generation, or set it to never ending.
Enable Notification	Select to enable report notification.
Output Profile	Select the output profile from the dropdown list, or click <i>Create New</i> to create a new output profile. See Output profiles on page 468 .

Filters section of Reports Settings tab

See [Filtering report output on page 454](#).

Advanced Settings section of Reports Settings tab

The following options are available in the *Advanced Settings* section of the *Settings* tab.

Field	Description
Language	Select the report language. Select one of the following: <i>Default</i> , <i>English</i> , <i>French</i> , <i>Japanese</i> , <i>Korean</i> , <i>Portuguese</i> , <i>Simplified_Chinese</i> , <i>Spanish</i> , or <i>Traditional_Chinese</i> .
Bundle rest into “Others”	Select to bundle the uncategorized results into an <i>Others</i> category.
Print Orientation	Set the print orientation to portrait or landscape.
Chart Heading Level	Set the heading level for the chart heading.
Default Font	Set the default font.
Hide # Column	Select to hide the column numbers.
Layout Header	Enter header text and select the header image. Accept the default Fortinet image or click <i>Browse</i> to select a different image.
Layout Footer	Select either the default footer or click <i>Custom</i> to enter custom footer text in the text field.
Print Cover Page	Select to print the report cover page. Click <i>Customize</i> to customize the cover page. See Customizing report cover pages on page 449 .

Field	Description
Print Table of Contents	Select to include a table of contents.
Print Device List	Select to print the device list. Select <i>Compact</i> , <i>Count</i> , or <i>Detailed</i> from the dropdown list.
Print Report Filters	Select to print the filters applied to the report.
Obfuscate User	Select to hide user information in the report.
Resolve Hostname	Select to resolve hostnames in the report.
Allow Save Maximum	Select a value between 1-10000 for the maximum number of reports to save.
Color Code	The color used to identify the report on the calendar. Select a color code from the dropdown list to apply to the report schedule. Color options include: <i>Bold Blue</i> , <i>Blue</i> , <i>Turquoise</i> , <i>Green</i> , <i>Bold Green</i> , <i>Yellow</i> , <i>Orange</i> , <i>Red</i> , <i>Bold Red</i> , <i>Purple</i> , and <i>Gray</i> .

Customizing report cover pages

A report cover page is only included in the report when enabled on the *Settings* tab in the *Advanced Settings* section. When enabled, the cover page can be customized to contain the desired information and imagery.

To customize a report cover page:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the toolbar.
4. Select the *Settings* tab and then click *Advanced Settings*.
5. Select the *Print Cover Page* checkbox, then click *Customize* next to the checkbox. The *Edit Cover Page* pane opens.

Edit Cover Page

Background Image: def_cove...png

Top Image:

Top Image Position:

Text Color:

☒ Show Creation Time

☒ Show Data Range

Report Title:

Custom Text 1:

Custom Text 2:

Bottom Image:

Footer Left Text:

Footer Right Text:

Footer Background Color:

6. Configure the following settings:

Background Image	Click <i>Browse</i> to open the <i>Choose an Image</i> dialog box. Select an image or click <i>Upload File</i> to find an image on the management computer, then click <i>OK</i> to add the image as the background image of the cover page.
Top Image	Click <i>Browse</i> to open the <i>Choose an Image</i> dialog box. Select an image or click <i>Upload File</i> to find an image on the management computer, then click <i>OK</i> to add the image at the top of the cover page.
Top Image Position	Select the top image position from the dropdown menu. Select one of the following: <i>Left</i> , <i>Center</i> , <i>Right</i> .
Text Color	Select a text color from the dropdown list.
Show Creation Time	Select to print the report date on the cover page.
Show Data Range	Select to print the data range on the cover page.
Report Title	Accept the default title or type another title in the <i>Report Title</i> field.
Custom Text 1	If you want, enter custom text for the <i>Custom Text 1</i> field.
Custom Text 2	If you want, enter custom text for the <i>Custom Text 2</i> field.
Bottom Image	Click <i>Browse</i> to open the <i>Choose an Image</i> dialog box. Select an image or click <i>Upload File</i> to find an image on the management computer, then click <i>OK</i> to add the image to the bottom of the cover page.
Footer Left Text	If you want, enter custom text to be printed in the left footer of the cover page.
Footer Right Text	If you want, enter custom text to be printed in the right footer of the cover page.
Footer Background Color	Select the cover page footer background color from the dropdown list.
Reset to Default	Select to reset the cover page settings to their default settings.

7. Click *OK* to save the configurations and return to the *Settings* tab.

Reports Layout tab



Because the cut, copy, and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

The following options are available in the *Layout* tab (layout editor):

Field	Description
Insert Chart or Edit Chart	<p>Click to insert a FortiManager chart. Charts are associated with datasets that extract data from logs for the report.</p> <p>In the <i>Insert Chart</i> or <i>Chart Properties</i> dialog box, you can specify a custom title, width, and filters for the chart. For information on setting filters, see Filtering report output on page 454.</p> <p>You can edit a chart by right clicking the chart in the layout editor and selecting <i>Chart Properties</i> or by clicking the chart to select it and then clicking <i>Edit Chart</i>.</p>
Insert Macro	Click to insert a FortiManager macro. Macros are associated with datasets that extract data from logs for the report.
Image	Click the <i>Image</i> button in the toolbar to insert an image into the report layout. Right-click an existing image to edit image properties.
Table	Click the <i>Table</i> button in the toolbar to insert a table into the report layout. Right-click an existing table to edit a cell, row, column, table properties, or delete the table.
Insert Horizontal Line	Click to insert a horizontal line.
Insert Page Break for Printing	Click to insert a page break for printing.
Link	Click the <i>Link</i> button in the toolbar to open the <i>Link</i> dialog box. You can select to insert a URL, a link to an anchor in the text, or an email address. Alternatively, use the <i>CTRL+L</i> keyboard shortcut to open the <i>Link</i> dialog box.
Anchor	Click the <i>Anchor</i> button in the toolbar to insert an anchor in the report layout.
Cut	<p>To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods:</p> <ul style="list-style-type: none"> Click the cut button in the toolbar Right-click and select cut in the menu Use the <i>CTRL+X</i> shortcut on your keyboard.
Copy	<p>To cut a text fragment, start with selecting it. When the text is selected, you can cut it using one of the following methods:</p> <ul style="list-style-type: none"> Click the cut button in the toolbar Right-click and select cut in the menu Use the <i>CTRL+C</i> shortcut on your keyboard.
Paste	To paste text, start with cutting or copying from another source. Depending on the security settings of your browser, you may either paste directly from the clipboard or use the <i>Paste</i> dialog box.
Paste as plain text	Click <i>Paste as plain text</i> to paste formatted text without the formatting. If the browser blocks the editor toolbar's access to clipboard, a <i>Paste as Plain Text</i> dialog box appears and you can paste the fragment into the text box using the <i>CTRL+V</i> keyboard shortcut.

Field	Description
Paste from Word	<p>You can preserve basic formatting when you paste a text fragment from Microsoft Word. To achieve this, copy the text in a Word document and paste it using one of the following methods:</p> <ul style="list-style-type: none"> Click the <i>Paste from Word</i> button in the toolbar Use the <i>CTRL+V</i> shortcut on your keyboard.
Undo	Click to undo the last action. Alternatively, use the <i>CTRL+Z</i> keyboard shortcut to perform the undo operation.
Redo	Click to redo the last action. Alternatively, use the <i>CTRL+Y</i> keyboard shortcut to perform the redo operation.
Find	<p>Click to find text in the report layout editor. This dialog box includes the following elements:</p> <ul style="list-style-type: none"> <i>Find what</i>: Is the text field where you enter the word or phrase you want to find. <i>Match case</i>: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means the search becomes case-sensitive. <i>Match whole word</i>: Checking this option limits the search operation to whole words. <i>Match cyclic</i>: Checking this option means that after the editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Replace	<p>Click to replace text in the report layout editor. This dialog box includes consists of the following elements:</p> <ul style="list-style-type: none"> <i>Find what</i>: Is the text field where you enter the word or phrase you want to find. <i>Replace with</i>: Is the text field where you enter the word or phrase that will replace the search term in the document. <i>Match case</i>: Checking this option limits the search operation to words whose case matches the spelling (uppercase and lowercase letters) given in the search field. This means the search becomes case-sensitive. <i>Match whole word</i>: Checking this option limits the search operation to whole words. <i>Match cyclic</i>: Checking this option means that after the editor reaches the end of the document, the search continues from the beginning of the text. This option is checked by default.
Save as Template	Click to save the layout as a template.
Paragraph Format	Select the paragraph format from the dropdown list. Select one of the following: <i>Normal</i> , <i>Heading 1</i> , <i>Heading 2</i> , <i>Heading 3</i> , <i>Heading 4</i> , <i>Heading 5</i> , <i>Heading 6</i> , <i>Formatted</i> , <i>Address</i> , or <i>Normal (DIV)</i> .
Font Name	Select the font from the dropdown list.

Field	Description
Font Size	Select the font size from the dropdown list. Select a size ranging from 8 to 72.
Bold	Select the text fragment and then click the <i>Bold</i> button in the toolbar. Alternatively, use the <i>CTRL+B</i> keyboard shortcut to apply bold formatting to a text fragment.
Italic	Select the text fragment and then click the <i>Italic</i> button in the toolbar. Alternatively, use the <i>CTRL+I</i> keyboard shortcut to apply italics formatting to a text fragment.
Underline	Select the text fragment and then click the <i>Underline</i> button in the toolbar. Alternatively, use the <i>CTRL+U</i> keyboard shortcut to apply underline formatting to a text fragment.
Strike Through	Select the text fragment and then click the <i>Strike Through</i> button in the toolbar.
Subscript	Select the text fragment and then click the <i>Subscript</i> button in the toolbar.
Superscript	Select the text fragment and then click the <i>Superscript</i> button in the toolbar.
Text Color	You can change the color of text in the report by using a color palette. To choose a color, select a text fragment, click the <i>Text Color</i> button in the toolbar, and select a color.
Background Color	You can also change the color of the text background.
Insert/Remove Numbered List	Click to insert or remove a numbered list.
Insert/Remove Bulleted List	Click to insert or remove a bulleted list.
Decrease Indent	To decrease the indentation of the element, click the <i>Decrease Indent</i> toolbar button. The indentation of a block-level element containing the cursor will decrease by one tabulator length.
Increase Indent	To increase the indentation of the element, click the <i>Increase Indent</i> toolbar button. The block-level element containing the cursor will be indented with one tabulator length.
Block Quote	Block quote is used for longer quotations that are distinguished from the main text by left and right indentation. It is recommended to use this type of formatting when the quoted text consists of several lines or at least 100 words.
Align Left	When you align your text left, the paragraph is aligned with the left margin and the text is ragged on the right side. This is usually the default text alignment setting for the languages with left to right direction.
Center	When you center your text, the paragraph is aligned symmetrically along the vertical axis and the text is ragged on the both sides. This setting is often used in titles or table cells.

Field	Description
Align Right	When you align your text right, the paragraph is aligned with the right margin and the text is ragged on the left side. This is usually the default text alignment setting for the languages with right to left direction.
Justify	When you justify your text, the paragraph is aligned to both the left and right margins and the text is not ragged on either side..
Remove Format	Click to remove formatting.

Filtering report output

You can apply log message filters to reports. You can set up report filters in one of the following areas:

- *Settings* tab *Filters* section.
- *Layout* tab *Filters* section in the *Insert Chart* or *Chart Properties* dialog box. To open this dialog box, click *Insert Chart* or *Edit Chart*, or right-click a chart and select *Chart Properties*.

In the *Filters* section, the following options are available.

Field	Description
Log messages that match	Available in the <i>Settings</i> tab only. Select <i>All</i> to filter log messages based on all of the added conditions, or select <i>Any of the Following Conditions</i> to filter log messages based on any one of the conditions.
Add Filter	Click to add filters. For each filter, select the field, and operator from the dropdown lists, then enter or select the values as applicable. Filters vary based on device type.
LDAP Query	Available in the <i>Settings</i> tab only. Click to add an LDAP query, then select the <i>LDAP Server</i> and the <i>Case Change</i> value from the dropdown lists. Use this option to query an LDAP server for group membership. The results of this query is used to filter the report to only match logs for users belonging to that group. You must specify the group name in the filter definition. If you enable <i>LDAP Query</i> , the group name is not used to match the group field in logs. The group name is only used for the LDAP query to determine group membership.

Managing reports

You can manage reports by going to *Reports > Report Definitions > All Reports*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a report to display the menu.

Option	Description
Create New	Creates a new report. You can choose whether to base the new report on a report template.
Edit	Edits the selected report.
Delete	Deletes the selected report.
Clone	Clones the selected report.
Run report	Generates a report.
Folder	Organizes reports into folders.
Import	Imports a report from a management computer.
Export	Exports a report to a management computer.
Show Scheduled Only	Filters the list to include only reports that have been run or are scheduled to be run.

Organizing reports into folders

You can create folders to organize reports.

To organize reports into folders:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. Click *Folder* in the toolbar, and select *Create New Folder*.
4. Specify the folder name and location and click *OK*. The folder is now displayed in the report list.

You can now create, clone, or import reports into this folder.

Importing and exporting reports

You can transport a report between FortiManager units. You can export a report from the FortiManager unit to the management computer. The report is saved as a .dat file on the management computer. You can then import the report file to another FortiManager unit.



Exporting reports only exports the report layout, charts, datasets, and images. Other report configurations are not exported.

To export reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.

3. In the content pane, select a report, and select *More > Export* in the toolbar to save the file to the management computer.

To import reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, click *More > Import* in the toolbar. The *Import Report* dialog box opens.
4. Drag and drop the report file onto the dialog box, or click *Browse* and locate the file to be imported on your local computer.
5. Select a folder to save the report to from the dropdown list.
6. Click OK to import the report.

Report template library



Because the cut, copy, and paste functions need access to the clipboard of your operating system, some Internet browsers either block it when called from the layout editor toolbar, or ask you to explicitly agree to it. If you're blocked from accessing the clipboard by clicking the respective cut, copy and paste buttons from the toolbar or context menu, you can always use keyboard shortcuts.

A report template defines the charts and macros that are in the report, as well as the layout of the content.

You can use the following items to create a report template:

- Text
- Images
- Tables
- Charts that reference datasets
- Macros that reference datasets

Datasets for charts and macros specify what data are used from the Analytics logs when you generate the report. You can also create custom charts and macros for use in report templates.

Creating report templates

You can create a report template by saving a report as a template or by creating a totally new template.

To create a report template:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Reports > Report Definitions > Templates*.
3. In the toolbar of the content pane, click *Create New*.

4. Set the following options:
 - a. Name
 - b. Description
 - c. Category
5. Use the toolbar to insert and format text and graphics for the template. In particular, use the *Insert Chart* and *Insert Macro* buttons to insert charts and macros into the template.

For a description of the fields, see [Reports Layout tab on page 450](#). For information about creating charts and macros, see [Creating charts on page 460](#) and [Creating macros on page 463](#).
6. Click *OK*.

The new template is now displayed on the template list.

To create a report template by saving a report:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > All Reports*.
3. In the content pane, select the report from the list, and click *Edit* in the toolbar.
4. In the *Layout* tab, click the *Save As Template* button in the toolbar.
5. In the *Save as Template* dialog box, set the following options, and click *OK*:
 - a. Name
 - b. Description
 - c. Category

The new template is now displayed on the template list.

Viewing sample reports for predefined report templates

You can view sample reports for predefined report templates to help you visualize how the reports would look.

To view sample reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to the *Reports > Report Definitions > Templates*.
3. In the content pane, click the *HTML* or *PDF* link in the *Preview* column of a template to view a sample report based on the template.

Managing report templates

You can manage report templates in *Reports > Report Definitions > Templates*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a template to display the menu.

Option	Description
Create New	Creates a new report template
Edit	Edits a report template. You can edit report templates that you created. You cannot edit predefined report templates.

Option	Description
View	Displays the settings for the predefined report template. You can copy elements from the report template to the clipboard, but you cannot edit a predefined report template.
Delete	Deletes the selected report template. You cannot delete predefined report templates.
Clone	Clones the selected report template
Rename	Renames the selected report template. You cannot rename predefined report templates.

List of report templates

FortiManager includes report templates you can use as is or build upon when you create a new report. FortiManager provide different templates for different devices.

You can find report templates in *Reports > Report Definitions > Templates*.

FortiGate report templates

Template - 360-Degree Security Review	Template - Security Analysis
Template - Admin and System Events Report	Template - Threat Report
Template - Application Risk and Control	Template - Top 20 Categories and Applications (Session)
Template - Bandwidth and Applications Report	Template - Top 20 Category and Websites (Bandwidth)
Template - Client Reputation	Template - Top 20 Category and Websites (Session)
Template - Cyber Threat Assessment	Template - Top 500 Sessions by Bandwidth
Template - DNS Report	Template - Top Allowed and Blocked with Timestamps
Template - Data Loss Prevention Detailed Report	Template - User Detailed Browsing Log
Template - Detailed Application Usage and Risk	Template - User Security Analysis
Template - Email Report	Template - User Top 500 Websites by Bandwidth
Template - FortiClient Default Report	Template - User Top 500 Websites by Session
Template - FortiClient Vulnerability Scan Report	Template - VPN Report
Template - FortiGate Performance Statistics Report	Template - Web Usage Report
Template - GTP Report	Template - What is New Report
Template - Hourly Website Hits	Template - WiFi Network Summary

Template - IPS Report

Template - Wireless PCI Compliance

Template - PCI-DSS Compliance Review

Template - SaaS Application Usage Report

FortiCache report templates

Template - FortiCache Default Report

Template - FortiCache Security Analysis

Template - FortiCache Web Usage Report

FortiClient report templates

Template - FortiClient Default Report

Template - FortiClient Vulnerability Scan Report

FortiDDoS report templates

Template - FortiDDoS Default Report

FortiMail report templates

Template - FortiMail Analysis Report

Template - FortiMail Default Report

FortiSandbox report templates

Template - FortiSandbox Default Report

FortiWeb report templates

Template - FortiWeb Default Report

Template - FortiWeb Web Application Analysis Report

Chart library

Use the Chart library to create, edit, and manage your charts.

Creating charts



You can also create charts using the *Log View* Chart Builder. See [Creating charts on page 420](#).

To create charts:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Chart Library*.
3. Click *Create New* in the toolbar.

Create Chart

Name:

Description:

Dataset:

Resolve Hostname:

Chart Type:

Data Bindings: ☒ Regular ☐ Ranked ☐ Drilldown

Columns

[Click to add Column](#)

Column 1

Title:

Width: % (0 for Auto)

Data Binding **Format**

Column 2

Title:

Width: % (0 for Auto)

Data Binding **Format**

☒ Order By:

Show Top (0 for all results):

4. Configure the settings for the new chart. The following table provides a description for each setting.

Name	Enter a name for the chart.
Description	Enter a description of the chart.
Dataset	Select a dataset from the dropdown list. For more information, see Datasets on page 465 . Options vary based on device type.
Resolve Hostname	Select to resolve the hostname. Select one of the following: <i>Inherit</i> , <i>Enabled</i> , or <i>Disabled</i> .
Chart Type	Select a graph type from the dropdown list; one of: <i>Table</i> , <i>Bar</i> , <i>Pie</i> , <i>Line</i> , <i>Area</i> , <i>Donut</i> , or <i>Radar</i> . This selection affects the rest of the available selections.
Data Bindings	The data bindings vary depending on the chart type selected.

Table

Table Type	Select <i>Regular</i> , <i>Ranked</i> , or <i>Drilldown</i> .
Add Column	Select to add a column. Up to 15 columns can be added for a <i>Regular</i> table. <i>Ranked</i> tables have two columns, and <i>Drilldown</i> tables have three columns.
Columns	The following column settings must be set: <ul style="list-style-type: none"> • <i>Column Title</i>: Enter a title for the column. • <i>Width</i>: Enter the column width as a percentage. • <i>Data Binding</i>: Select a value from the dropdown list. The options vary depending on the selected dataset. • <i>Format</i>: Select a value from the dropdown list. • <i>Add Data Binding</i>: Add data bindings to the column. Every column must have at least one data binding. The maximum number varies depending on the table type.
Order By	Select what to order the table by. The available options vary depending on the selected dataset.
Show Top	Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the <i>Others</i> category for <i>Ranked</i> and <i>Drilldown</i> tables.
Drilldown Top	Enter a numerical value. Only the first 'X' items are displayed. This options is only available for <i>Drilldown</i> tables.

Bar

X-Axis	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Label</i>: Enter a label for the axis. • <i>Show Top</i>: Enter a numerical value. Only the first 'X' items are displayed. Other items are bundled into the <i>Others</i> category.
Y-axis	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Format</i>: Select a format from the dropdown list: <i>Bandwidth</i>, <i>Counter</i>, <i>Default</i>, <i>Percentage</i>, or <i>Severity</i>. • <i>Label</i>: Enter a label for the axis.
Bundle rest into "Others"	Select to bundle the rest of the results into an <i>Others</i> category.
Group By	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Show Top</i>: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the <i>Others</i> category.
Order By	Select to order by the X-Axis or Y-Axis.

Pie, Donut, or Radar

Category	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Label</i>: Enter a label for the axis. • <i>Show Top</i>: Enter a numerical value. Only the first 'X' items are displayed. Other items can be bundled into the <i>Others</i> category.
Series	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Format</i>: Select a format from the dropdown list: <i>Bandwidth</i>, <i>Counter</i>, <i>Default</i>, <i>Percentage</i>, or <i>Severity</i>. • <i>Label</i>: Enter a label for the axis.
Bundle rest into "Others"	Select to bundle the rest of the results into an <i>Others</i> category.
Line or Area	
X-Axis	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Label</i>: Enter a label for the axis.
Lines	<ul style="list-style-type: none"> • <i>Data Binding</i>: Select a value from the dropdown list. The available options vary depending on the selected dataset. • <i>Format</i>: Select a format from the dropdown list: <i>Bandwidth</i>, <i>Counter</i>, <i>Default</i>, <i>Percentage</i>, or <i>Severity</i>. • <i>Type</i>: Select the type from the dropdown list: <i>Line Up</i> or <i>Line Down</i>. • <i>Legend</i>: Enter the legend text for the line.
Add line	Select to add more lines.

5. Click **OK**.

Managing charts

Manage your charts in *Reports > Report Definitions > Chart Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a chart to display the menu.

Option	Description
Create New	Creates a new chart.
Edit	Edits a chart. You can edit charts that you created. You cannot edit predefined charts.
View	Displays the settings for the selected predefined chart. You cannot edit a predefined chart.
Delete	Deletes the selected chart. You can delete charts that you create. You cannot delete predefined charts.

Option	Description
Clone	Clones the selected chart.
Import	Imports a previously exported FortiManager chart.
Export	Exports one or more FortiManager charts.
Show Predefined	Displays the predefined charts.
Show Custom	Displays the custom charts.
Search	Lets you search for a chart name.

Viewing datasets associated with charts

To view datasets associated with charts:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Chart Library*.
3. Select a chart, and click *View* in the toolbar.
4. In the *View Chart* pane, find the name of the dataset associated with the chart in the *Dataset* field.
5. Go to *Reports > Report Definitions > Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Select the dataset that is found, and click *View* in the toolbar to view it.

Macro library

Use the Macro library to create, edit, and manage your macros.

Creating macros

FortiManager includes a number of predefined macros. You can also create new macros, or clone and edit existing macros.

Macros are predefined to use specific datasets and queries. They are organized into categories, and can be added to, removed from, and organized in reports.



Macros are currently supported in FortiGate and FortiCarrier ADOMs only.

To create a new macro:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Macro Library*, and click *Create New*. The *Create Macro* pane is displayed.

Create Macro

Name

Description

Dataset

App-Risk-App-Usage-By-Category

Query

select appcat, sum(coalesce(sentbyte, 0)+coalesce(rcvbyte, 0)) as bandwidth from \$log where \$filter and logid_to_int(logid) not in (4, 7, 14) and nullifna(appcat) is not null group by appcat order by bandwidth desc

Data Binding

appcat

Display

Text

OK

Cancel

3. Provide the required information for the new macro.

Name	Enter a name for the macro.
Description	Enter a description of the macro.
Dataset	Select a dataset from the dropdown list. The options will vary based on device type.
Query	Displays the query statement for the dataset selected.
Data Binding	The data bindings vary depending on the dataset selected. Select a data binding from the dropdown list.
Display	Select a value from the dropdown list.

4. Click *OK*. The newly created macro is shown in the Macro library.

Managing macros

You can manage macros by *Reports > Report Definitions > Macro Library*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a macro to display the menu.

Option	Description
Create New	Creates a new macro.
Edit	Edits the selected macro. You can edit macros that you created. You cannot edit predefined macros.
View	Displays the settings for the selected macro. You cannot edit a predefined macro.
Delete	Deletes the selected macro. You can delete macros that you create. You cannot delete predefined macros.
Clone	Clones the selected macro.
Show Predefined	Displays the predefined macros.

Option	Description
Show Custom	Displays the custom macros.
Search	Lets you search for a macro name.

Viewing datasets associated with macros

To view datasets associated with macros:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Macro Library*.
3. Select a macro, and click *View* (for predefined macros) or *Edit* (for custom macros) in the toolbar.
4. In the *View Macro* or *Edit Macro* pane, find the name of the dataset associated with the macro in the *Dataset* field.
5. Go to *Reports > Report Definitions > Datasets*.
6. In the *Search* box, type the name of the dataset.
7. Double-click the dataset to view it.

Datasets

Use the Datasets pane to create, edit, and manage your datasets.

Creating datasets

FortiManager datasets are collections of data from logs for monitored devices. Charts and macros reference datasets. When you generate a report, the datasets populate the charts and macros to provide data for the report.

Predefined datasets for each supported device type are provided, and new datasets can be created and configured.

To create a new dataset:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Datasets*, and click *Create New*. The *Create Dataset* pane is displayed.
3. Provide the required information for the new dataset.

Name	Enter a name for the dataset.
-------------	-------------------------------

Log Type	<p>Select a log type from the dropdown list.</p> <ul style="list-style-type: none"> The following log types are available for FortiGate: <i>Application Control, Intrusion Prevention, Content Log, Data Leak Prevention, Email Filter, Event, Traffic, Virus, VoIP, Web Filter, Vulnerability Scan, FortiClient Event, FortiClient Traffic, FortiClient Vulnerability Scan, Web Application Firewall, GTP, DNS, and Local Event.</i> The following log types are available for FortiMail: <i>Email Filter, Event, History, and Virus.</i> The following log types are available for FortiWeb: <i>Intrusion Prevention, Event, and Traffic.</i>
Query	Enter the SQL query used for the dataset. An easy way to build a custom query is to copy and modify a predefined dataset's query.
Variables	Click the <i>Add</i> button to add variable, expression, and description information.
Test query with specified devices and time period	
Time Period	Use the dropdown list to select a time period. When selecting <i>Custom</i> , enter the start date and time, and the end date and time.
Devices	Select <i>All Devices</i> or <i>Specify</i> to select specific devices to run the SQL query against. Click the <i>Select Device</i> button to add multiple devices to the query.
Test	Click to test the SQL query before saving the dataset configuration.

4. Click *Test*.

The query results are displayed. If the query is not successful, an error message appears in the *Test Result* pane.

5. Click *OK*.

Viewing the SQL query for an existing dataset

You can view the SQL query for a dataset, and test the query against specific devices or all devices.

To view the SQL query for an existing dataset:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Report Definitions > Datasets*.
3. Hover the mouse cursor over the dataset on the dataset list. The SQL query is displayed as a tooltip.
You can also open the dataset to view the *Query* field.

SQL query functions

In addition to standard SQL queries, the following are some SQL functions specific to FortiAnalyzer. These are based on standard SQL functions.

<code>root_domain(hostname)</code>	<p>The root domain of the FQDN. An example of using this function is:</p> <pre>select devid, root_domain(hostname) as website FROM \$log WHERE 'user'='USER01' GROUP BY devid, hostname ORDER BY hostname LIMIT 7</pre>
<code>nullifna(expression)</code>	<p>This is the inverse operation of <code>coalesce</code> that you can use to filter out n/a values. This function takes an expression as an argument. The actual SQL syntax this is based on is <code>select nullif(nullif(expression, 'N/A'), 'n/a')</code>.</p> <p>In the following example, if the user is n/a, the source IP is returned, otherwise the username is returned.</p> <pre>select coalesce(nullifna('user'), nullifna('srcip')) as user_ src, coalesce(nullifna(root_domain(hostname)), 'unknown') as domain FROM \$log WHERE dstport='80' GROUP BY user_src, domain ORDER BY user_src LIMIT 7</pre>
<code>email_domain</code> <code>email_user</code>	<p><code>email_domain</code> returns the text after the @ symbol in an email address. <code>email_user</code> returns the text before the @ symbol in an email address. An example of using this function is:</p> <pre>select 'from' as source, email_user('from') as e_user, email_ domain('from') as e_domain FROM \$log LIMIT 5 OFFSET 10</pre>
<code>from_dtime</code> <code>from_itime</code>	<p><code>from_dtime(bigint)</code> returns the device timestamp without time zone. <code>from_itime(bigint)</code> returns FortiAnalyzer's timestamp without time zone. An example of using this function is:</p> <pre>select itime, from_itime(itime) as faz_local_time, dtime, from_ dtime(dtime) as dev_local_time FROM \$log LIMIT 3</pre>

Managing datasets

You can manage datasets by going to *Reports > Report Definitions > Datasets*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a dataset to display the menu.

Option	Description
Create New	Creates a new dataset.
Edit	Edits the selected dataset. You can edit datasets that you created. You cannot edit predefined datasets.
View	Displays the settings for the selected dataset. You cannot edit predefined datasets.
Delete	Deletes the selected dataset. You can delete datasets that you create. You cannot delete predefined datasets.

Option	Description
Clone	Clones the selected dataset. You can edit cloned datasets.
Validate	Validate selected datasets.
Validate All Custom	Validates all custom datasets.
Search	Lets you search for a dataset name.

Output profiles

Output profiles allow you to define email addresses to which generated reports are sent and provide an option to upload the reports to FTP, SFTP, or SCP servers. Once created, an output profile can be specified for a report.

Creating output profiles



You must configure a mail server before you can configure an output profile. See [Mail Server on page 518](#).

To create output profiles:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Advanced > Output Profile*.
3. Click *Create New*. The *Create Output Profile* pane is displayed.

Create Output Profile

Name

test

Comments

Output Format

☒ PDF
☐ HTML
☐ XML
☐ CSV

☒ Email Generated Reports

Subject

Body

Recipients

Email Server

fortinet: smtp.fortinet.com

From

test@fortinet.com

To

test@fortinet.com

+

☒ Upload Report to Server

Server Type

FTP

Server

0.0.0.0

User

Password

Directory

☐ Delete file(s) after uploading

OK

Cancel

4. Provide the following information, and click **OK**:

Name	Enter a name for the new output profile.
Comments	Enter a comment about the output profile (optional).
Output Format	Select the format or formats for the generated report. You can choose <i>PDF</i> , <i>HTML</i> , <i>XML</i> , or <i>CSV</i> format.
Email Generated Reports	Enable emailing of generated reports.
Subject	Enter a subject for the report email.
Body	Enter body text for the report email.
Recipients	Select the email server from the dropdown list and enter to and from email addresses. Click <i>Add</i> to add another entry so that you can specify multiple recipients.
Upload Report to Server	Enable uploading of generated reports to a server.
Server Type	Select <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> from the dropdown list.
Server	Enter the server IP address.
User	Enter the username.
Password	Enter the password.
Directory	Specify the directory where the report will be saved.
Delete file(s) after uploading	Select to delete the generated report after it has been uploaded to the selected server.

Managing output profiles

You can manage output profiles by going to *Reports > Advanced > Output Profile*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click an output profile to display the menu.

Option	Description
Create New	Creates a new output profile.
Edit	Edits the selected output profile.
Delete	Deletes the selected output profile.

Report languages

You can specify the language of reports when creating a report. You can add new languages, and you can change the name and description of the languages. You cannot edit the predefined languages.

Predefined report languages

FortiManager includes the following predefined report languages:

- English (default report language)
- French
- Japanese
- Korean
- Portuguese
- Simplified Chinese
- Spanish
- Traditional Chinese

Adding language placeholders

To add a language placeholder:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Advanced > Language*.
3. Click *Create New* in the toolbar.
4. In the *New Language* pane, enter a name and description for the language, and click *OK*.
A new language placeholder is created.



Adding a new language placeholder does not create that language. It only adds a placeholder for that language that contains the language name and description.

Managing report languages

You can manage report languages by going to *Reports > Advanced > Language*. Some options are available as buttons on the toolbar. Some options are available in the right-click menu. Right-click a language to display the menu.

Option	Description
Create New	Creates a new report language placeholder.
View	Views details about the selected report language.
Edit	Edits the selected report language. You cannot edit predefined report languages.
Delete	Deletes the selected report language. You cannot delete predefined report languages.

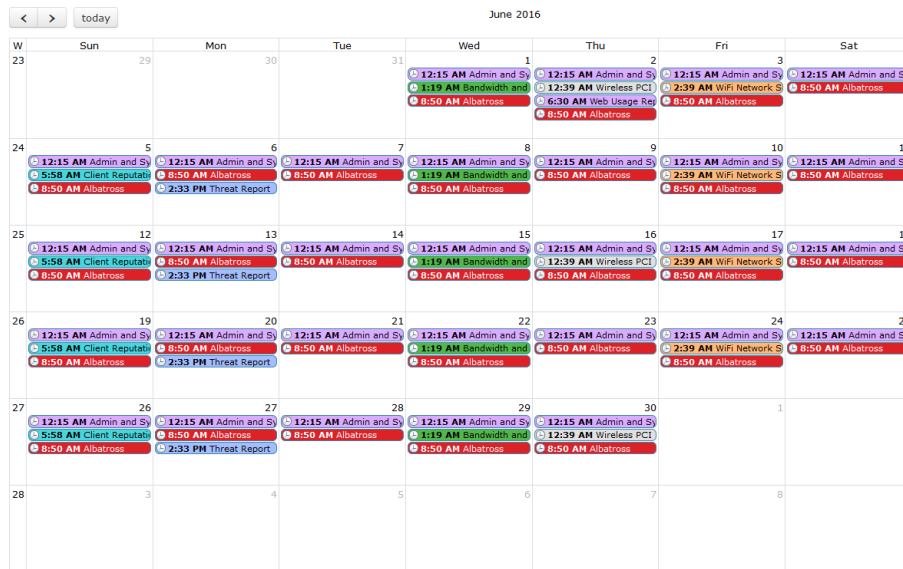
Report calendar

You can use the report calendar to view all the reports that are scheduled for the selected month. You can edit or disable upcoming report schedules, as well as delete or download completed reports.

Viewing all scheduled reports

To view all scheduled reports:

1. If using ADOMs, ensure you are in the correct ADOM.
2. Go to *Reports > Advanced > Report Calendar*.



3. Hover the mouse cursor over a calendar entry to display the name, status, and device type of the scheduled report.
4. Click a generated report to download it.
5. Click a scheduled report to go to the *Settings* tab of the report.
6. Click the left or right arrow at the top of the *Report Calendar* pane to change the month that is displayed. Click *Today* to return to the current month.

Managing report schedules

You can manage report schedules in *Reports > Advanced > Report Calendar*.

To edit a report schedule:

1. In *Report Calendar*, right-click an upcoming calendar entry, and select *Edit*.
2. In the Settings tab of the report that opens, edit the corresponding report schedule.

To disable a report schedule:

In *Report Calendar*, right-click an upcoming calendar entry, and select *Disable*. All scheduled instances of the report are removed from the report calendar. Completed reports remain in the report calendar.

To delete or download a completed report:

In *Report Calendar*, right-click a past calendar entry, and select *Delete* or *Download*. The corresponding completed report will be deleted or downloaded.



You can only delete or download scheduled reports that have a *Finished* status. You cannot delete scheduled reports with a *Pending* status.

System Settings

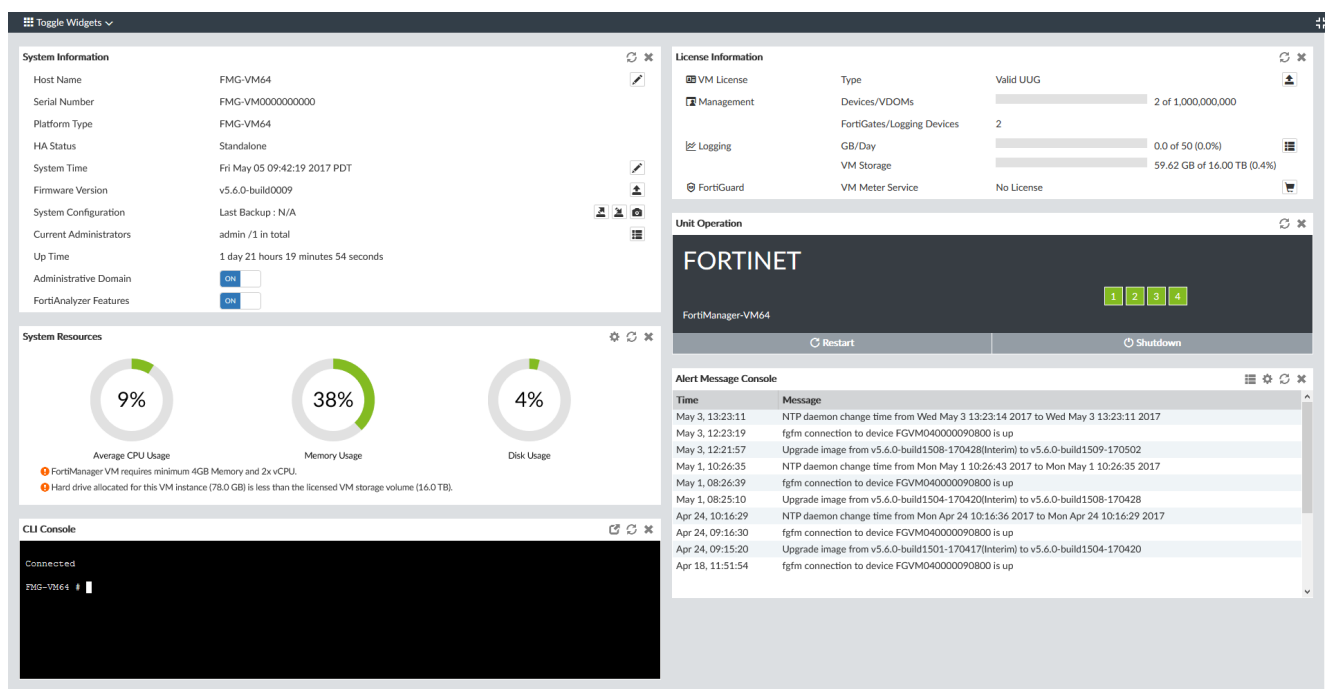
System Settings allows you to manage system options for your FortiManager device.



Additional configuration options and short-cuts are available using the right-click menu. Right-click the mouse on different navigation panes on the GUI page to access these options.

Dashboard

The *Dashboard* contains widgets that provide performance and status information and enable you to configure basic system settings. The dashboard also contains a CLI widget that lets you use the command line through the GUI.



The following widgets are available:

Widget	Description
System Information	<p>Displays basic information about the FortiManager system, such as up time and firmware version. You can also enable or disable Administrative Domains and FortiAnalyzer features. For more information, see System Information widget on page 475.</p> <p>From this widget you can manually update the FortiManager firmware to a different release. For more information, see Updating the system firmware on page 478.</p> <p>The widget fields will vary based on how the FortiManager is configured, for example, if ADOMs are enabled.</p>
System Resources	<p>Displays the real-time and historical usage status of the CPU, memory and hard disk. For more information, see System Resources widget on page 481.</p>
License Information	<p>Displays the devices being managed by the FortiManager unit and the maximum numbers of devices allowed. For more information, see License Information widget on page 482.</p> <p>From this widget you can manually upload a license for VM systems.</p>
Unit Operation	<p>Displays status and connection information for the ports of the FortiManager unit. It also enables you to shutdown and restart the FortiManager unit or reformat a hard disk. For more information, see Unit Operation widget on page 483.</p>
CLI Console	<p>Opens a terminal window that enables you to configure the FortiManager unit using CLI commands directly from the GUI. For more information, see CLI Console widget on page 483.</p>
Alert Message Console	<p>Displays log-based alert messages for both the FortiManager unit and connected devices. For more information, see Alert Messages Console widget on page 484.</p>
Log Receive Monitor	<p>Displays a real-time monitor of logs received. You can view data per device or per log type. For more information, see Log Receive Monitor widget on page 484.</p> <p>The <i>Log Receive Monitor</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.</p>
Insert Rate vs Receive Rate	<p>Displays the log insert and receive rates. For more information, see Insert Rate vs Receive Rate widget on page 485.</p> <p>The <i>Insert Rate vs Receive Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.</p>
Log Insert Lag Time	<p>Displays how many seconds the database is behind in processing the logs. For more information, see Log Insert Lag Time widget on page 485.</p> <p>The <i>Log Insert Lag Time</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.</p>

Widget	Description
Receive Rate vs Forwarding Rate	Displays the <i>Receive Rate</i> , which is the rate at which FortiManager is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server. For more information, see Receive Rate vs Forwarding Rate widget on page 486 . The <i>Receive Rate vs Forwarding Rate</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.
Disk I/O	Displays the disk utilization, transaction rate, or throughput as a percentage over time. For more information, see Disk I/O widget on page 486 . The <i>Disk I/O</i> widget is available when <i>FortiAnalyzer Features</i> is enabled.

Customizing the dashboard

The FortiManager system dashboard can be customized. You can select which widgets to display, where they are located on the page, and whether they are minimized or maximized. It can also be viewed in full screen by selecting the full screen button on the far right side of the toolbar.

Action	Steps
Move a widget	Move the widget by clicking and dragging its title bar, then dropping it in its new location
Add a widget	Select <i>Toggle Widgets</i> from the toolbar, then select the name widget you need to add.
Delete a widget	Click the <i>Close</i> icon in the widget's title bar.
Customize a widget	For widgets with an edit icon, you can customize the widget by clicking the Edit icon and configuring the settings.
Reset the dashboard	Select <i>Toggle Widgets > Reset to Default</i> from the toolbar. The dashboards will be reset to the default view.

System Information widget

The information displayed in the *System Information* widget is dependent on the FortiManager models and device settings. The following information is available on this widget:

Host Name	The identifying name assigned to this FortiManager unit. Click the edit host name button to change the host name. For more information, see Changing the host name on page 476 .
Serial Number	The serial number of the FortiManager unit. The serial number is unique to the FortiManager unit and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Platform Type	Displays the FortiManager platform type, for example <i>FMGVM64</i> (virtual machine).

HA Status	Displays if FortiManager unit is in High Availability mode and whether it is the Master or Slave unit in the HA cluster. For more information see High Availability on page 488 .
System Time	The current time on the FortiManager internal clock. Click the edit system time button to change system time settings. For more information, see Configuring the system time on page 477 .
Firmware Version	The version number and build number of the firmware installed on the FortiManager unit. To update the firmware, you must download the latest version from the Customer Service & Support website at https://support.fortinet.com . Click the update button, then select the firmware image to load from the local hard disk or network volume. For more information, see Updating the system firmware on page 478 .
System Configuration	The date of the last system configuration backup. The following actions are available: <ul style="list-style-type: none"> Click the backup button to backup the system configuration to a file; see Backing up the system on page 479. Click the restore to restore the configuration from a backup file; see Restoring the configuration on page 479. You can also migrate the configuration to a different FortiManager model by using the CLI. See Migrating the configuration on page 480. Click the check point to revert the system to a prior saved configuration; see System checkpoints on page 480.
Current Administrators	The number of administrators currently logged in. Click the current session list button to view the session details for all currently logged in administrators.
Up Time	The duration of time the FortiManager unit has been running since it was last started or restarted.
Administrative Domain	Displays whether ADOMs are enabled. Toggle the switch to change the Administrative Domain state. See Enabling and disabling the ADOM feature on page 54 .
FortiAnalyzer Features	Displays whether FortiAnalyzer features are enabled. Toggle the switch to change the FortiAnalyzer features state. <i>FortiAnalyzer Features</i> are not available on available on the FortiManager 100C. See FortiAnalyzer Features on page 390 for information.

Changing the host name

The host name of the FortiManager unit is used in several places.

- It appears in the *System Information* widget on the dashboard. For more information about the *System Information* widget.
- It is used in the command prompt of the CLI.
- It is used as the SNMP system name.

The *System Information* widget and the `get system status` CLI command will display the full host name. However, if the host name is longer than 16 characters, the CLI and other places display the host name in a truncated form ending with a tilde (~) to indicate that additional characters exist, but are not displayed. For example, if the host name is FortiManager1234567890, the CLI prompt would be FortiManager123456~#.

To change the host name:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the edit host name button next to the *Host Name* field.
3. In the *Host Name* box, type a new host name.
The host name may be up to 35 characters in length. It may include US-ASCII letters, numbers, hyphens, and underscores. Spaces and special characters are not allowed.
4. Click the checkmark to change the host name.

Configuring the system time

You can either manually set the FortiManager system time or configure the FortiManager unit to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.



For many features to work, including scheduling, logging, and SSL-dependent features, the FortiManager system time must be accurate.

To configure the date and time:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the edit system time button next to the *System Time* field.
3. Configure the following settings to either manually configure the system time, or to automatically synchronize the FortiManager unit's clock with an NTP server:

System Time	The date and time according to the FortiManager unit's clock at the time that this pane was loaded or when you last clicked the <i>Refresh</i> button.
Time Zone	Select the time zone in which the FortiManager unit is located and whether or not the system automatically adjusts for daylight savings time.
Update Time By	Select <i>Set time</i> to manually set the time, or <i>Synchronize with NTP Server</i> to automatically synchronize the time.
Set Time	Manually set the data and time.
Select Date	Set the date from the calendar or by manually entering it in the format: YYYY/MM/DD.
Select Time	Select the time.
Synchronize with NTP Server	Automatically synchronize the date and time.

Sync Interval	Enter how often, in minutes, the device should synchronize its time with the NTP server. For example, entering 1440 causes the Fortinet unit to synchronize its time once a day.
Server	Enter the IP address or domain name of an NTP server. Click the plus icon to add more servers. To find an NTP server that you can use, go to http://www.ntp.org .

- Click the checkmark to apply your changes.

Updating the system firmware

To take advantage of the latest features and fixes, FortiManager provides two ways to upgrade its firmware: manually or through the FDN. For information about upgrading your FortiManager device, see the *FortiManager Upgrade Guide*, or contact Fortinet Customer Service & Support.



Backup the configuration and database before changing the firmware of your FortiManager unit. Changing the firmware to an older or incompatible version may reset the configuration and database to the default values for that firmware version, resulting in data loss. For information on backing up the configuration, see [Backing up the system on page 479](#).



Before you can download firmware updates for your FortiManager unit, you must first register your FortiManager unit with Customer Service & Support. For details, go to <https://support.fortinet.com/> or contact Customer Service & Support.

To manually update the FortiManager firmware:

- Download the firmware (the .out file) from the Customer Service & Support website, <https://support.fortinet.com/>.
- Go to *System Settings > Dashboard*.
- In the *System Information* widget, in the *Firmware Version* field, click *Upgrade Firmware*. The *Firmware Upload* dialog box opens.
- Drag and drop the file onto the dialog box, or click *Browse* to locate the firmware package (.out file) that you downloaded from the Customer Service & Support portal and then click *Open*.
- Click *OK*. Your device will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.



Optionally, you can upgrade firmware stored on an FTP or TFTP server using the following CLI command:

```
execute restore image {ftp | tftp} <file path to server> <IP of server> <username on server> <password>
```

For more information, see the [FortiManager CLI Reference](#).

- Refresh the browser and log back into the device.

7. Launch the *Device Manager* module and make sure that all formerly added devices are still listed.
8. Launch other functional modules and make sure they work properly.



Installing firmware replaces the current network vulnerability management engine with the version included with the firmware release that you are installing. After you install the new firmware, make sure that your vulnerability definitions are up-to-date. For more information, see [FortiGuard on page 353](#).

The FortiManager firmware can also be updated through the FDN. For more information, see [Firmware images on page 373](#).

Backing up the system

Fortinet recommends that you back up your FortiManager configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal affect to the network. You should also perform a back up after making any changes to the FortiManager configuration or settings that affect the connected devices.

You can perform backups manually or at scheduled intervals. You can also create a backups - called checkpoints - that define a point where the FortiManager and network management is stable and functioning. Should any future configurations cause issues, you have a point where the system is stable.

Fortinet recommends backing up all configuration settings from your FortiManager unit before upgrading the FortiManager firmware.

To back up the FortiManager configuration:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the backup button next to *System Configuration*. The *Backup System* dialog box opens
3. If you want to encrypt the backup file, select the *Encryption* box, then type and confirm the password you want to use. The password can be a maximum of 63 characters.
4. Select *OK* and save the backup file on your management computer.

Restoring the configuration

You can use the following procedure to restore your FortiManager configuration from a backup file on your management computer.

If your FortiManager unit is in HA mode, switch to Standalone mode.



The restore operation will temporarily disable the communication channel between FortiManager and all managed devices. This is a safety measure, in case any devices are being managed by another FortiManager. To re-enable the communication, please go to *System Settings > Advanced > Advanced Settings* and disable *Offline Mode*.

To restore the FortiManager configuration:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the restore button next to *System Configuration*. The *Restore System* dialog box opens.
3. Configure the following settings then select *OK*.

Choose Backup File	Select <i>Browse</i> to find the configuration backup file you want to restore, or drag and drop the file onto the dialog box.
Password	Type the encryption password, if applicable.
Overwrite current IP, routing and HA settings	Select the checkbox to overwrite the current IP, routing, and HA settings.
Restore in Offline Mode	Informational checkbox. Hover over the help icon for more information.

Migrating the configuration

You can back up the system of one FortiManager model, and then use the CLI and the FTP, SCP, or SFTP protocol to migrate the settings to another FortiManager model.

You need the username and password for the FortiManager model to which you are migrating the configuration file.

If you encrypted the FortiManager configuration file when you created it, you need the password to decrypt the configuration file when you migrate the file to another FortiManager model.

To migrate the FortiManager configuration:

1. In one FortiManager model, go to *System Settings > Dashboard*.
2. Back up the system. See [Backing up the system on page 479](#).
3. In the other FortiManager model, go to *System Settings > Dashboard*.
4. In the *CLI Console* widget, type the following command:

```
execute migrate all-settings <ftp | scp | sftp> <server> <filepath> <user> <password>
[cryptpasswd]
```

System checkpoints

You can create a system checkpoint backup to capture a specific configuration. This backup provides a history where the FortiManager and FortiGate units are completely in sync. Should there be a major failure, you can completely revert the FortiManager to when it was in working order. These are, in essence, snapshots of your FortiManager managed network system.

You should make a system checkpoint backup before installing new firmware to devices or making a major configuration change to the network. If the update or modification causes problems, you can quickly revert to an earlier known “good” version of the configuration to restore operation.

A system checkpoint backup includes the system configuration of the FortiManager unit.

Please note the following:

- The system checkpoint does not include the FortiGate settings.
- For policy package specific settings, after reverting to a checkpoint, you need to re-install policy packages to update FortiGate policy and related configuration.
- For non-policy package settings, after reverting to a checkpoint, you must trigger FortiGate to auto-update and overwrite the checkpoint reverted configuration. Alternatively, you can disable the auto update function in System Settings and re-install the checkpoint reverted configuration to FortiGate.

To create a system checkpoint:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the checkpoint button next to *System Configuration*. The *System Checkpoint List* opens.
3. Select *Create New*. The *Add New System Checkpoint* dialog box opens.
4. In the *Comments* box, type a description, up to 63 characters, for the reason or state of the backup.
5. Select *OK*. The system checkpoint task will be run and the checkpoint will be created.

To revert to a system checkpoint:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the checkpoint button next to *System Configuration*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table then click *Revert*.
4. A confirmation dialog box will open. Select *OK* to continue.



When reverting to a system checkpoint, the FortiManager will reboot.

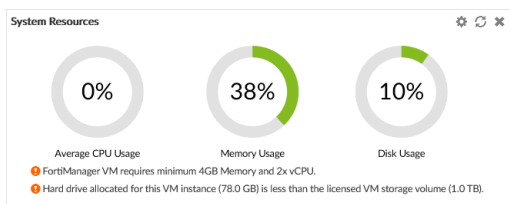
To delete a system checkpoint:

1. Go to *System Settings > Dashboard*.
2. In the *System Information* widget, click the checkpoint button next to *System Configuration*. The *System Checkpoint* table opens.
3. Select the system checkpoint in the table then select *Delete* in the toolbar.
4. Click *OK* in the confirmation dialog box to delete the checkpoint.

System Resources widget

The *System Resources* widget displays the usage status of the CPUs, memory, and hard disk. You can view system resource information in real-time or historical format, as well as average or individual CPU usage.

On VMs, warning messages are displayed if the amount of memory or the number of CPUs assigned are too low, or if the allocated hard drive space is less than the licensed amount. These warnings are also shown in the notification list (see [GUI overview on page 34](#)). Clicking on a warning opens the [FortiManager VM Install Guide](#).



To toggle between real-time and historical data, click *Edit* in the widget toolbar, select *Historical* or *Real-time*, edit the other settings as required, then click *OK*.

To view individual CPU usage, from the Real-Time display, click on the CPU chart. To go back to the standard view again, click the chart again.

License Information widget

The *License Information* widget displays the number of devices connected to the FortiManager.

License Information		
VM License	Type	Valid UUG
Management	Devices/VDOMs	5 of 1,000,000,000
	FortiGates/Logging Devices	5
	FortiAPs	26
FortiGuard	VM Meter Service	No License
	Server Location	Global Servers
Update Server	AntiVirus and IPS	288.88.888.88 (Cmnmam, BC, Canada)
	Web and Email Filter	188.888.888.885 (Snmnmnm, CA, United States)
	FortiClient Update	88.88.88.885 (Snmnmnm, CA, United States)

VM License

VM license information and status.

Click the upload license button to upload a new VM license file.

This field is only visible for FortiManager VM.

Management

Device/VDOMs

The total number of devices and VDOMs connected to the FortiManager and the total number of device and VDOM licenses.

FortiGates/Logging Devices

The number of connected FortiGates and other logging devices.

FortiAPs

The number of connected FortiAPs.

Logging

This section is only shown when *FortiAnalyzer Features* is enabled. For more information, see [FortiAnalyzer Features on page 390](#).

GB/Day

The gigabytes per day of logs allowed and used for this FortiManager. Click the show details button to view the GB per day of logs used for the previous 6 days.

VM Storage

The amount of VM storage used and remaining.
This field is only visible for FortiManager VM.

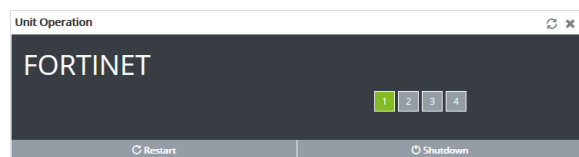
FortiGuard

VM Meter Service	The license status. Click the purchase button to go to the Fortinet Customer Service & Support website, where you can purchase a license.
Secure DNS Server	The SDNS server license status. Click the upload image button to upload a license key.
Server Location	The locations of the FortiGuard servers, either global or US only. Click the edit icon to adjust the location. Changing the server location will cause the FortiManager to reboot.
Update Server	
AntiVirus and IPS	The IP address and physical location of the Antivirus and IPS update server.
Web and Email Filter	The IP address and physical location of the web and email filter update server.
FortiClient Update	The IP address and physical location of the FortiClient update server.

Unit Operation widget

The *Unit Operation* widget graphically displays the status of each port. The port name indicates its status by its color. Green indicates the port is connected. Grey indicates there is no connection.

Hover the cursor over the ports to view a pop-up that displays the full name of the interface, the IP address and netmask, the link status, the speed of the interface, and the amounts of sent and received data.



CLI Console widget

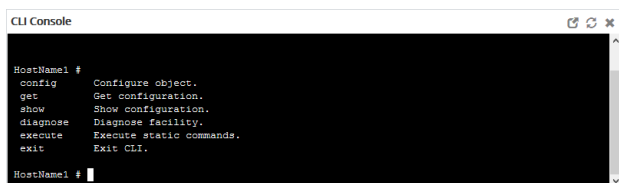
The *CLI Console* widget enables you to type command lines through the GUI, without making a separate Telnet, SSH, or local console connection to access the CLI.



The *CLI Console* widget requires that your web browser support JavaScript.

For information on available CLI commands, see the [FortiManager CLI Reference](#).

When using the *CLI Console* widget, you are logged in with the same administrator account you used to access the GUI. You can enter commands by typing them, or you can copy and paste commands into or out of the console.



```

CLI Console
HostName1 #
config      Configure object.
get         Get configuration.
show        Show configuration.
diagnose    Diagnose facility.
execute     Execute static commands.
exit        Exit CLI.
HostName1 #

```

Click *Detach* in the widget toolbar to open the widget in a separate window.

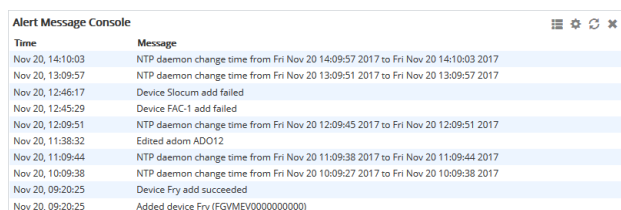
Alert Messages Console widget

The *Alert Message Console* widget displays log-based alert messages for both the FortiManager unit itself and connected devices.

Alert messages help you track system events on your FortiManager unit such as firmware changes, and network events such as detected attacks. Each message shows the date and time the event occurred.



Alert messages can also be delivered by email, syslog, or SNMP.



Time	Message
Nov 20, 14:10:03	NTP daemon change time from Fri Nov 20 14:09:57 2017 to Fri Nov 20 14:10:03 2017
Nov 20, 13:09:57	NTP daemon change time from Fri Nov 20 13:09:51 2017 to Fri Nov 20 13:09:57 2017
Nov 20, 12:46:17	Device Slocum add failed
Nov 20, 12:45:29	Device FAC-1 add failed
Nov 20, 12:09:51	NTP daemon change time from Fri Nov 20 12:09:45 2017 to Fri Nov 20 12:09:51 2017
Nov 20, 11:38:32	Edited adom ADO12
Nov 20, 11:09:44	NTP daemon change time from Fri Nov 20 11:09:38 2017 to Fri Nov 20 11:09:44 2017
Nov 20, 10:09:38	NTP daemon change time from Fri Nov 20 10:09:27 2017 to Fri Nov 20 10:09:38 2017
Nov 20, 09:20:25	Device Fry add succeeded
Nov 20, 09:20:25	Added device Fry (FGVMEV0000000000)

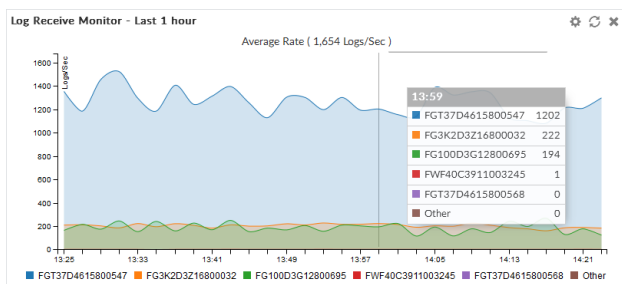
Click *Edit* from the widget toolbar to view the *Alert Message Console Settings*, where you can adjust the number of entries that are visible in the widget, and the refresh interval.

To view a complete list of alert messages, click *Show More* from the widget toolbar. The widget will show the complete list of alerts. To clear the list, click *Delete All Messages*. Click *Show Less* to return to the previous view.

Log Receive Monitor widget

The *Log Receive Monitor* widget displays the rate at which the FortiManager unit receives logs over time. Log data can be displayed by either log type or device.

Hover the cursor over a point on the graph to see the exact number of logs that were received at a specific time. Click the name of a device or log type to add or remove it from the graph. Click *Edit* in the widget toolbar to modify the widget's settings.



This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

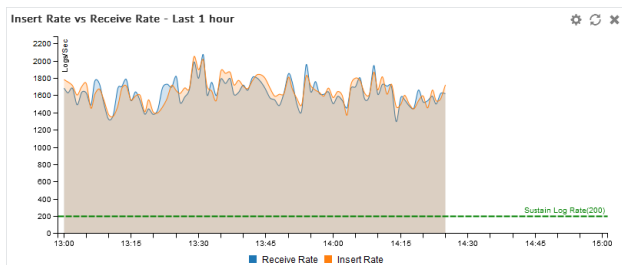
Insert Rate vs Receive Rate widget

The *Insert Rate vs Receive Rate* widget displays the log insert and log receive rates over time.

- Log receive rate: how many logs are being received.
- Log insert rate: how many logs are being actively inserted into the database.

If the log insert rate is higher than the log receive rate, then the database is rebuilding. The lag is the number of logs waiting to be inserted.

Hover the cursor over a point on the graph to see the exact number of logs that were received and inserted at a specific time. Click *Receive Rate* or *Insert Rate* to remove those data from the graph. Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval.

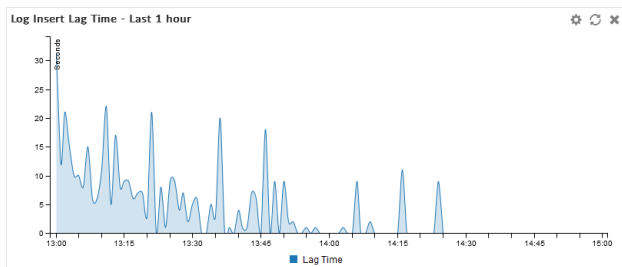


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Log Insert Lag Time widget

The *Log Insert Lag Time* widget displays how many seconds the database is behind in processing the logs.

Click the edit icon in the widget toolbar to adjust the time interval shown on the graph and the refresh interval (0 to disable) of the widget.

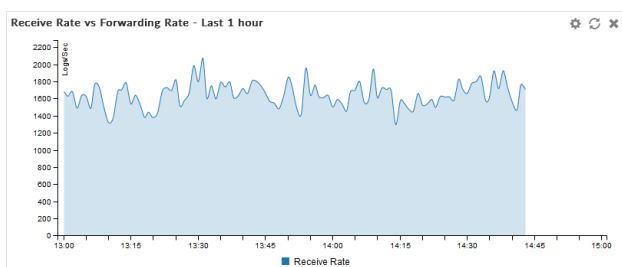


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Receive Rate vs Forwarding Rate widget

The *Receive Rate vs Forwarding Rate* widget displays the rate at which the FortiManager is receiving logs. When log forwarding is configured, the widget also displays the log forwarding rate for each configured server.

Click the edit icon in the widget toolbar to adjust the time period shown on the graph and the refresh interval, if any, of the widget.

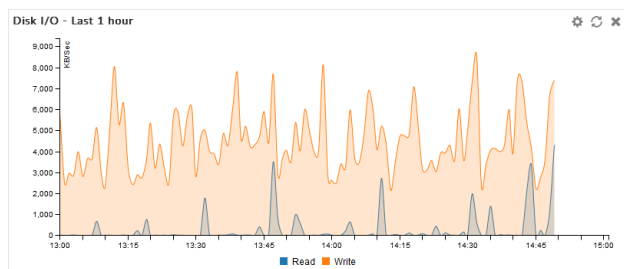


This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Disk I/O widget

The *Disk I/O* widget shows the disk utilization (%), transaction rate (requests/s), or throughput (KB/s), versus time.

Click the edit icon in the widget toolbar to select which chart is displayed, the time period shown on the graph, and the refresh interval (if any) of the chart.



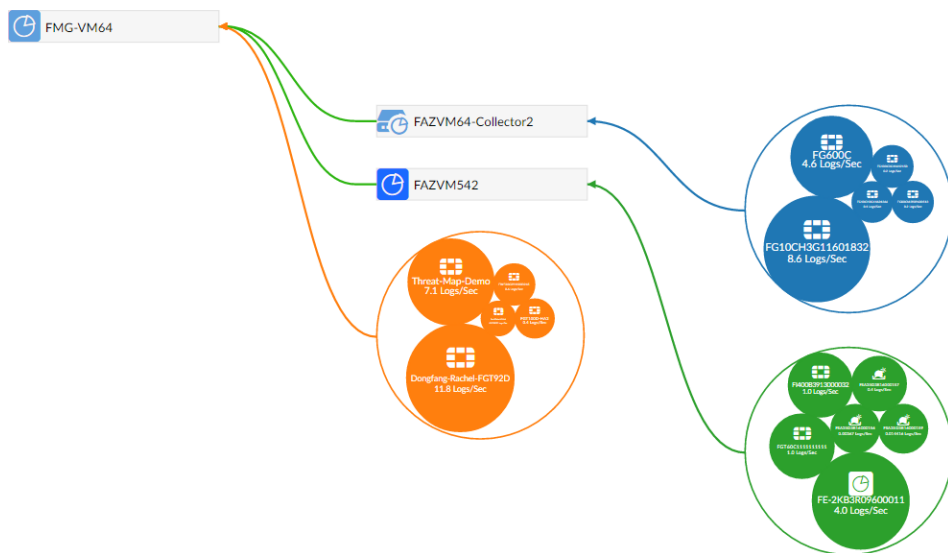
This widget is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features](#) on page 390.

Logging Topology

The *Logging Topology* pane shows the physical topology of devices in the security fabric. Click, hold, and drag to adjust the view in the content pane, and double-click or use the scroll wheel to change the zoom.

The visualization can be filtered to show only FortiAnalyzer devices or all devices by device count or traffic.

Hovering the cursor over a device in the visualization will show information about the device, such as the IP address and device name. Right-click on a device and select *View Related Logs* to go to the *Log View* pane, filtered for that device.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features](#) on page 390.

High Availability

FortiManager high availability (HA) provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability. Understanding what's required for FortiManager reliability begins with understanding what normal FortiManager operations are and how to make sure normal operations continue if a FortiManager unit fails.

Most of the FortiManager operations involve storing FortiManager and FortiGate configuration and related information in the FortiManager database on the FortiManager unit hard disk. A key way to enhance reliability of FortiManager is to protect the data in the FortiManager database from being lost if the FortiManager unit fails. This can be achieved by dynamically backing up FortiManager database changes to one or more backup FortiManager units. Then, if the operating FortiManager unit fails, a backup FortiManager unit can take the place of the failed unit.

A FortiManager HA cluster consists of up five FortiManager units of the same FortiManager series. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup, or slave, units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example, over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. Managed devices connect with the primary unit for normal management operations (configuration push, auto-update, firmware upgrade, and so on). If FortiManager is used to distribute FortiGuard updates to managed devices, managed devices can connect to the primary FortiManager unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IP addresses as it did when it was the backup unit.



A reboot of the FortiManager device is not required when it is promoted from a backup to the primary unit.



When devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices will be used.

Synchronizing the FortiManager configuration and HA heartbeat

All changes to the FortiManager database are saved on the primary unit, and then these changes are synchronized to the backup units. The FortiManager configuration of the primary unit is also synchronized to the backup units (except for the HA parameters). As a result, the backup units always match the primary unit. So if the primary unit fails, a backup unit can be configured to take the place of the primary unit and continue functioning as a standalone FortiManager unit.

While the FortiManager cluster is operating, all backup units in the cluster exchange HA heartbeat packets with the primary unit so the primary unit can verify the status of the backup units and the backup units can verify the status of the primary unit. The HA heartbeat packets use TCP port 5199. HA heartbeat monitoring, as well as FortiManager database and configuration synchronization takes place using the connections between the FortiManager units in the cluster. As part of configuring the primary unit you add peer IPs and peer serial numbers of each of the backup FortiManager units

in the cluster. You also add the peer IP of the primary unit and the primary unit serial number to each of the backup units.



Depending on the peer IPs that you use, you can isolate HA traffic to specific FortiManager interfaces and connect those interfaces together so they function as synchronization interfaces between the FortiManager units in the cluster. Communication between the units in the cluster must be maintained for the HA cluster to operate.

The interfaces used for HA heartbeat and synchronization communication can be connected to your network. However, if possible you should isolate HA heartbeat and synchronization packets from your network to save bandwidth.

If the primary or a backup unit fails

If the primary unit fails the backup units stop receiving HA heartbeat packets from the primary unit. If one of the backup units fails, the primary unit stops receiving HA heartbeat packets from the backup unit. In either case the cluster is considered down until it is reconfigured.

When the cluster goes down the cluster units still operating send SNMP traps and write log messages to alert the system administrator that a failure has occurred. You can also see the failure from the *HA Status* page.

You re-configure the cluster by removing the failed unit from the cluster configuration. If the primary unit has failed, this means configuring one of the backup units to be the primary unit and adding peer IPs for all of the remaining backup units to the new primary unit configuration.

If a backup unit has failed, you re-configure the cluster by removing the peer IP of the failed backup unit from the primary unit configuration.

Once the cluster is re-configured it will continue to operate as before but with fewer cluster units. If the failed unit is restored you can re-configure the cluster again to add the failed unit back into the cluster. In the same way you can add a new unit to the cluster by changing the cluster configuration to add it.

FortiManager HA cluster startup steps

FortiManager units configured for HA start up begin sending HA heartbeat packets to their configured peer IP addresses and also begin listening for HA heartbeat packets from their configured peer IP addresses.

When the FortiManager units receive HA heartbeat packets with a matching HA cluster ID and password from a peer IP address, the FortiManager unit assumes the peer is functioning.

When the primary unit is receiving HA heartbeat packets from all of the configured peers or backup units, the primary unit sets the cluster status to up. Once the cluster is up the primary unit then synchronizes its configuration to the backup unit. This synchronization process can take a few minutes depending on the size of the FortiManager database. During this time database and configuration changes made to the primary unit are not synchronized to the backup units. Once synchronization is complete, if changes were made during synchronization, they are re-synchronized to the backup units.

Most of the primary unit configuration, as well as the entire FortiManager database, are synchronized to the backup unit. Interface settings and HA settings are not synchronized. These settings must be configured on each cluster unit.


Once the synchronization is complete, the FortiManager HA cluster begins normal operation.




Configuring HA options

To configure HA options go to *System Settings > HA*. From here you can configure FortiManager units to start an HA cluster or you can change the HA configuration of the cluster.

To configure a cluster, you must set the mode of the primary unit to *Master* and the modes of the backup units to *Slave*. Then you must add the IP addresses and serial numbers of each backup unit to primary unit peer list. The IP address and serial number of the primary unit must be added to each of the backup unit HA configurations. Also, the primary unit and all backup units must have the same *Cluster ID* and *Group Password*.

You can connect to the primary unit GUI to work with FortiManager. Thanks to configuration synchronization, you can configure and work with the cluster in the same way as you would work with a standalone FortiManager unit.

Cluster Status (Master Mode )

SN	Mode	IP	Enable	Module Data Synchronized	Pending Module Data
 FMG-VM0000000000	Master	Connecting to Peer		-	-
 FMG-VM1000203004	Slave	10.10.10.11		0.0 KB	0.0 KB

Cluster Settings

Operation Mode: Standalone **Master** Slave

Peer IP: IPv4 10.10.10.11 Peer SN: FMG-VM1000203004 + -

Cluster ID: 2 (1-64)

Group Password:

File Quota: 4096 (2048-20480) MB

Heart Beat Interval: 5 Seconds

Fallover Threshold: 3 (1-255)

Download Debug Log: Download

Apply

Configure the following settings:

Cluster Status	Monitor FortiManager HA status. See Monitoring HA status on page 494 .
SN	The serial number of the device.
Mode	The high availability mode, either <i>Master</i> or <i>Slave</i> .
IP	The IP address of the device.
Enable	Shows if the peer is currently enabled.
Module Data Synchronized	Module data synchronized in bytes.
Pending Module Data	Pending module data in bytes.
Cluster Settings	
Operation Mode	Select <i>Master</i> to configure the FortiManager unit to be the primary unit in a cluster. Select <i>Slave</i> to configure the FortiManager unit to be a backup unit in a cluster. Select <i>Standalone</i> to stop operating in HA mode.

Peer IP	Select the peer IP version from the dropdown list, either <i>IPv4</i> or <i>IPv6</i> . Then, type the IP address of another FortiManager unit in the cluster. For the primary unit you can add up to four Peer IP addresses for up to four backup units. For a backup unit you can only add the IP address of the primary unit.
Peer SN	Type the serial number of the FortiManager unit corresponding to the entered IP address.
Cluster ID	A number between 1 and 64 that identifies the HA cluster. All members of the HA cluster must have the same cluster ID. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different cluster ID. The FortiManager GUI browser window title changes to include the cluster ID when FortiManager unit is operating in HA mode.
Group Password	A password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.
File Quota	Enter the file quota, from 2048 to 20480MB (default: 4096MB). You cannot configure the file quota for backup units.
Heart Beat Interval	The time a cluster unit waits between sending heartbeat packets, in seconds. The heartbeat interval is also the amount of time that a FortiManager unit waits before expecting to receive a heartbeat packet from the other cluster unit. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds. You cannot configure the heartbeat interval on the backup units.
Failover Threshold	<p>The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed. The default failover threshold is 3. The failover threshold range is 1 to 255. You cannot configure the failover threshold of the backup units.</p> <p>In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds.</p> <p>If the failure detection time is too short, the HA cluster may detect a failure when none has occurred. For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred.</p> <p>If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.</p>
Download Debug Log	Select to download the HA debug log file to the management computer.

General FortiManager HA configuration steps

1. Configure the FortiManager units for HA operation:
 - Configure the primary unit.
 - Configure the backup units.
2. Change the network configuration so the remote backup unit and the primary unit can communicate with each other.
3. Connect the units to their networks.
4. Add basic configuration settings to the cluster:
 - Add a password for the admin administrative account.
 - Change the IP address and netmask of the port1 interface.
 - Add a default route.

GUI configuration steps

Use the following procedures to configure the FortiManager units for HA operation from the FortiManager unit GUI. It assumes you are starting with three FortiManager units with factory default configurations. The primary unit and the first backup unit are connected to the same network. The second backup unit is connected to a remote network and communicates with the primary unit over the Internet. Sample configuration settings are also shown.

To configure the primary unit for HA operation:

1. Connect to the primary unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.

Example HA master configuration:

Operation Mode	Master
Peer IP	172.20.120.23
Peer SN	<serial_number>
Peer IP	192.268.34.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure the backup unit on the same network for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.

Example local backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	172.20.120.45
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To configure a remote backup unit for HA operation:

1. Connect to the backup unit GUI.
2. Go to *System Settings > HA*.
3. Configure HA settings.

Example remote backup configuration:

Operation Mode	Slave
Priority	5 (Keep the default setting.)
Peer IP	192.168.20.23
Peer SN	<serial_number>
Cluster ID	15
Group Password	password
File Quota	4096
Heartbeat Interval	5 (Keep the default setting.)
Failover Threshold	3 (Keep the default setting.)

4. Click *Apply*.

To change the network configuration so that the remote backup unit and the primary unit can communicate with each other:

Configure the appropriate firewalls or routers to allow HA heartbeat and synchronization traffic to pass between the primary unit and the remote backup unit using the peer IPs added to the primary unit and remote backup unit configurations.

HA traffic uses TCP port 5199.

To connect the cluster to the networks:

1. Connect the cluster units.
No special network configuration is required for the cluster.
2. Power on the cluster units.
The units start and use HA heartbeat packets to find each other, establish the cluster, and synchronize their configurations.

To add basic configuration settings to the cluster:

Configure the cluster to connect to your network as required.

Monitoring HA status

Go to *System Settings > HA* to monitor the status of the FortiManager units in an operating HA cluster. The FortiManager HA status pane displays information about the role of each cluster unit, the HA status of the cluster, and the HA configuration of the cluster.



The FortiManager GUI browser window title changes to indicate that the FortiManager unit is operating in HA mode. The following text is added to the title *HA (Group ID: <group_id>)*. Where <group_id> is the HA Group ID.



From the FortiManager CLI you can use the command `get system ha` to display the same HA status information.

The following information is displayed:

Cluster Status	The cluster status can be <i>Up</i> if this unit is received HA heartbeat packets from all of its configured peers. The cluster status will be <i>Down</i> if the cluster unit is not receiving HA heartbeat packets from one or more of its configured peers.
Mode	The role of the FortiManager unit in the cluster. The role can be: <ul style="list-style-type: none"> • <i>Master</i>: for the primary (or master) unit. • <i>Slave</i>: for the backup units.
Module Data Synchronized	The amount of data synchronized between this cluster unit and other cluster units.

Pending Module Data

The amount of data waiting to be synchronized between this cluster unit and other cluster units.

Upgrading the FortiManager firmware for an operating cluster

You can upgrade the firmware of an operating FortiManager cluster in the same way as upgrading the firmware of a standalone FortiManager unit. During the firmware upgrade procedure, you connect to the primary unit GUI or CLI to upgrade the firmware.

Similar to upgrading the firmware of a standalone FortiManager unit, normal FortiManager operations are temporarily interrupted while the cluster firmware upgrades. As a result of this interruption, you should only upgrade the firmware during a maintenance period.

To upgrade FortiManager HA cluster firmware:

1. Log into the primary unit GUI.
2. Upgrade the primary unit firmware.

The firmware is forwarded to all the slave units, and then all the devices (master and slaves) are rebooted.

See the *FortiManager Release Notes* and *FortiManager Upgrade Guide* in the [Fortinet Document Library](#) for more information.



Administrators may not be able to connect to the FortiManager GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI may also be slow; use the console to connect to the CLI.

Certificates

The FortiManager generates a certificate request based on the information you entered to identify the FortiManager unit. After you generate a certificate request, you can download the request to a management computer and then forward the request to a CA.

Local certificates are issued for a specific server, or website. Generally they are very specific, and often for an internal enterprise network.

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to an entire company.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and include the date and time when the next CRL will be issued, as well as a sequence number to help ensure you have the most current versions.

Local certificates

The FortiManager unit generates a certificate request based on the information you enter to identify the FortiManager unit. After you generate a certificate request, you can download the request to a computer that has management access to the FortiManager unit and then forward the request to a CA.

The certificate window also enables you to export certificates for authentication, importing, and viewing.

The FortiManager has one default local certificate: *Fortinet_Local*.

You can manage local certificates from the *System Settings > Certificates > Local Certificates* page. Some options are available in the toolbar. Some options are also available in the right-click menu.

Creating a local certificate

To create a certificate request:

1. Go to *System Settings > Certificates > Local Certificates*
2. Click *Create New* in the toolbar. The *Generate Certificate Signing Request* pane opens.
3. Enter the following information as required, then click *OK* to save the certificate request:

Certificate Name	The name of the certificate.
Subject Information	Select the ID type from the dropdown list: <ul style="list-style-type: none"> • <i>Host IP</i>: Select if the unit has a static IP address. Enter the public IP address of the unit in the <i>Host IP</i> field. • <i>Domain Name</i>: Select if the unit has a dynamic IP address and subscribes to a dynamic DNS service. Enter the domain name of the unit in the <i>Domain Name</i> field. • <i>Email</i>: Select to use an email address. Enter the email address in the <i>Email Address</i> field.
Optional Information	
Organization Unit (OU)	The name of the department. You can enter a series of OUs up to a maximum of 5. To add or remove an OU, use the plus (+) or minus (-) icons.
Organization (O)	Legal name of the company or organization.
Locality (L)	Name of the city or town where the device is installed.
State/Province (ST)	Name of the state or province where the FortiGate unit is installed.
Country (C)	Select the country where the unit is installed from the dropdown list.
E-mail Address (EA)	Contact email address.

Subject Alternative Name	<p>Optionally, enter one or more alternative names for which the certificate is also valid. Separate names with a comma.</p> <p>A name can be:</p> <ul style="list-style-type: none"> • e-mail address • IP address • URI • DNS name (alternatives to the Common Name) • directory name (alternatives to the Distinguished Name) <p>You must precede the name with the name type. Examples:</p> <ul style="list-style-type: none"> • IP:1.1.1.1 • email:test@fortinet.com • email:my@other.address • URI:http://my.url.here/
Key Type	The key type can be <i>RSA</i> or <i>Elliptic Curve</i> .
Key Size	Select the key size from the dropdown list: <i>512 Bit</i> , <i>1024 Bit</i> , <i>1536 Bit</i> , or <i>2048 Bit</i> . This option is only available when the key type is <i>RSA</i> .
Curve Name	Select the curve name from the dropdown list: <i>secp256r1</i> (default), <i>secp384r1</i> , or <i>secp521r1</i> . This option is only available when the key type is <i>Elliptic Curve</i> .
Enrollment Method	The enrollment method is set to <i>File Based</i> .

Importing local certificates

To import a local certificate:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Click *Import* in the toolbar or right-click and select *Import*. The *Import* dialog box opens.
3. Enter the following information as required, then click *OK* to import the local certificate:

Type	Select the certificate type from the dropdown list: <i>Local Certificate</i> , <i>PKCS #12 Certificate</i> , or <i>Certificate</i> .
Certificate File	Click <i>Browse...</i> and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
Key File	<p>Click <i>Browse...</i> and locate the key file on the management computer, or drag and drop the file onto the dialog box.</p> <p>This option is only available when <i>Type</i> is <i>Certificate</i>.</p>
Password	<p>Enter the certificate password.</p> <p>This option is only available when <i>Type</i> is <i>PKCS #12 Certificate</i> or <i>Certificate</i>.</p>

Certificate Name

Enter the certificate name.

This option is only available when *Type* is *PKCS #12 Certificate* or *Certificate*.

Deleting local certificates

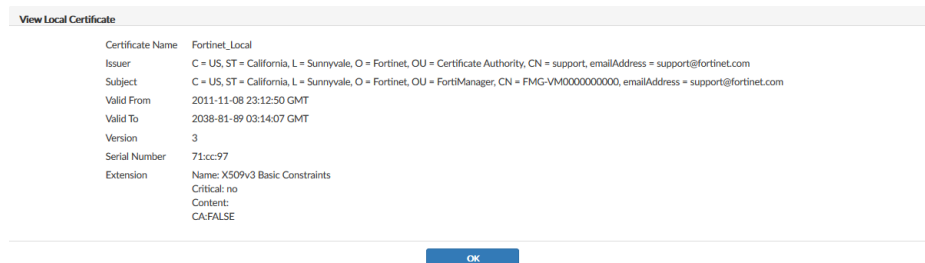
To delete a local certificate or certificates:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.

Viewing details of local certificates

To view details of a local certificate:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Select the certificates that you would like to see details about, then click *View Certificate Detail* in the toolbar or right-click menu. The *View Local Certificate* page opens.



3. Click *OK* to return to the local certificates list.

Downloading local certificates

To download a local certificate:

1. Go to *System Settings > Certificates > Local Certificates*.
2. Select the certificate that you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

CA certificates

The FortiManager has one default CA certificate, *Fortinet_CA*. In this sub-menu you can delete, import, view, and download certificates.

Importing CA certificates

To import a CA certificate:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
3. Click *Browse...* and locate the certificate file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the certificate.

Viewing CA certificate details

To view a CA certificate's details:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Select the certificates you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *View CA Certificate* page opens.
4. Click *OK* to return to the CA certificates list.

Downloading CA certificates

To download a CA certificate:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Select the certificate you need to download.
3. Click *Download* in the toolbar, or right-click and select *Download*, and save the certificate to the management computer.

Deleting CA certificates

To delete a CA certificate or certificates:

1. Go to *System Settings > Certificates > CA Certificates*.
2. Select the certificate or certificates you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected certificate or certificates.



The *Fortinet_CA* certificate cannot be deleted.

Certificate revocation lists

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA.

The CRL is a list of certificates that have been revoked and are no longer usable. This list includes expired, stolen, or otherwise compromised certificates. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiManager unit according to the procedures given below.

Importing a CRL

To import a CRL:

1. Go to *System Settings > Certificates > CRL*.
2. Click *Import* in the toolbar, or right-click and select *Import*. The *Import* dialog box opens.
3. Click *Browse...* and locate the CRL file on the management computer, or drag and drop the file onto the dialog box.
4. Click *OK* to import the CRL.

Viewing a CRL

To view a CRL:

1. Go to *System Settings > Certificates > CRL*.
2. Select the CRL you need to see details about.
3. Click *View Certificate Detail* in the toolbar, or right-click and select *View Certificate Detail*. The *Result* page opens.
4. Click *OK* to return to the CRL list.

Deleting a CRL

To delete a CRL or CRLs:

1. Go to *System Settings > Certificates > CRL*.
2. Select the CRL or CRLs you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected CRL or CRLs.

Fetcher Management

Log fetching is used to retrieve archived logs from one FortiManager device to another. This allows administrators to run queries and reports against historic data, which can be useful for forensic analysis.

The fetching FortiManager can query the server FortiManager and retrieve the log data for a specified device and time period, based on specified filters. The retrieved data are then indexed, and can be used for data analysis and reports.

Log fetching can only be done on two FortiManager devices running the same firmware. A FortiManager device can be either the fetch server or the fetching client, and it can perform both roles at the same time with different FortiManager devices. Only one log fetching session can be established at a time between two FortiManager devices.

The basic steps for fetching logs are:

1. On the client, create a fetching profile. See [Fetching profiles on page 501](#).
2. On the client, send the fetch request to the server. See [Fetch requests on page 502](#).
3. If this is the first time fetching logs with the selected profile, or if any changes have been made to the devices and/or ADOMs since the last fetch, on the client, sync devices and ADOMs with the server. See [Synchronizing devices and ADOMs on page 504](#).
4. On the server, review the request, then either approve or reject it. See [Request processing on page 504](#).
5. Monitor the fetch process on either FortiManager. See [Fetch monitoring on page 505](#).
6. On the client, wait until the database is rebuilt before using the fetched data for analysis.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Fetching profiles

Fetching profiles can be managed from the *Profiles* tab on the *System Settings > Fetcher Management* pane.

Profiles can be created, edited, and deleted as required. The profile list shows the name of the profile, as well as the IP address of the server it fetches from, the server and local ADOMs, and the administrator name on the fetch server.

To create a new fetching profile:

1. On the client, go to *System Settings > Fetcher Management*.
2. Select the *Profiles* tab, then click *Create New* in the toolbar, or right-click and select *Create New* from the menu. The *Create New Profile* dialog box opens.

Create New Profile

Name

Server IP

User

Password

3. Configure the following settings, then click *OK* to create the profile.

Name	Enter a name for the profile.
Server IP	Enter the IP address of the fetch server.
User	Enter the username of an administrator on the fetch server, which, together with the password, authenticates the fetch client's access to the fetch server.
Password	Enter the administrator's password, which, together with the username, authenticates the fetch client's access to the fetch server.



The fetch server administrator user name and password must be for an administrator with either a *Standard_User* or *Super_User* profile.

To edit a fetching profile:

1. Go to *System Settings > Fetching Management*.
2. Double-click on a profile, right-click on a profile then select *Edit*, or select a profile then click *Edit* in the toolbar. The *Edit Profile* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete a fetching profile or profiles:

1. Go to *System Settings > Fetching Management*.
2. Select the profile or profiles you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected profile or profiles.

Fetch requests

A fetch request requests archived logs from the fetch server configured in the selected fetch profile. When making the request, the ADOM on the fetch server the logs are fetched from must be specified. An ADOM on the fetching client must be specified or, if needed, a new one can be created. If logs are being fetched to an existing local ADOM, you must ensure the ADOM has enough disk space for the incoming logs.

The data policy for the local ADOM on the client must also support fetching logs from the specified time period. It must keep both archive and analytics logs long enough so they will not be deleted in accordance with the policy. For example: Today is July 1, the ADOM's data policy is configured to keep analytics logs for 30 days (June 1 - 30), and you need to fetch logs from the first week of May. The data policy of the ADOM must be adjusted to keep analytics and archive logs for at least 62 days to cover the entire time span. Otherwise, the fetched logs will be automatically deleted after they are fetched.

To send a fetch request:

1. On the fetch client, go to *System Settings > Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Request Fetch* in the toolbar, or right-click and select *Request Fetch* from the menu. The *Fetch Logs* dialog box opens.

Fetch Logs

Name

FAZVM64

Server IP

222.222.222.222

User

admino

Secure Connection

☒

Server ADOM

root

Local ADOM

root

Devices

FortiGate-VM64

Select Device +

Enable Filters

☐

Time Period

2017/01/30

09

10

2017/02/04

09

10

Index Fetched Logs

☒

Request Fetch

Cancel

3. Configure the following settings, then click *Request Fetch*.

The request is sent to the fetch server. The status of the request can be viewed in the *Sessions* tab.

Name	Displays the name of the fetch server you have specified.
Server IP	Displays the IP address of the server you have specified.
User	Displays the username of the server administrator you have provided.
Secure Connection	Select to use SSL connection to transfer fetched logs from the server.
Server ADOM	Select the ADOM on the server the logs will be fetched from. Only one ADOM can be fetched from at a time.
Local ADOM	Select the ADOM on the client where the logs will be received. Either select an existing ADOM from the dropdown list, or create a new ADOM by entering a name for it into the field.
Devices	Add the devices the logs will be fetched from. Up to 256 devices can be added. Click <i>Select Device</i> , select devices from the list, then click <i>OK</i> .
Enable Filters	Select to enable filters on the logs that will be fetched. Select <i>All</i> or <i>Any of the Following Conditions</i> in the <i>Log messages that match</i> field to control how the filters are applied to the logs. Add filters to the table by selecting the <i>Log Field</i> , <i>Match Criteria</i> , and <i>Value</i> for each filter.
Time Period	Specify what date and time range of log messages to fetch.
Index Fetch Logs	If selected, the fetched logs will be indexed in the SQL database of the client once they are received. Select this option unless you want to manually index the fetched logs.

Synchronizing devices and ADOMs

If this is the first time the fetching client is fetching logs from the device, or if any changes have been made the devices or ADOMs since the last fetch, then the devices and ADOMs must be synchronized with the server.

To synchronize devices and ADOMs:

1. On the client, go to *System Settings > Fetcher Management* and select the *Profiles* tab
2. Select the profile then click *Sync Devices* in the toolbar, or right-click and select *Sync Devices* from the menu. The *Sync Server ADOM(s) & Device(s)* dialog box opens and shows the progress of the process.

Once the synchronization is complete, you can verify the changes on the client. For example, newly added devices in the ADOM specified by the profile.



If a new ADOM is created, the new ADOM will mirror the disk space and data policy of the corresponding server ADOM. If there is not enough space on the client, the client will create an ADOM with the maximum allowed disk space and give a warning message. You can then adjust disk space allocation as required.

Request processing

After a fetching client has made a fetch request, the request will be listed on the fetch server in the *Received Request* section of the *Sessions* tab on the *Fetcher Management* pane. It will also be available from the notification center in the GUI banner.

Fetch requests can be approved or rejected.

To process the fetch request:

1. Go to the notification center in the GUI banner and click the log fetcher request, or go to the *Sessions* tab on the *System Settings > Fetcher Management* pane.

Expand All Collapse All				
Request Time	Host/Server IP	User	Status	Action
Received Request(1)				
15:01:55	FAZVM64(FAZ-VM0000000001)	admino	Waiting for approval	Review
Fetch Request(1)				

2. Find the request in the *Received Request* section. You may have to expand the section, or select *Expand All* in the content pane toolbar. The status of the request will be *Waiting for approval*.

3. Click *Review* to review the request. The *Review Request* dialog box will open.

Review Request

Host Name

FAZVM64

Serial No.

FAZ-VM0000000000

Version

v5.6.0

User

Agg

Devices

ADOM	Device	VDOM
root	FGVMEV0000000000	*

Filters

None

Time Period

16:02 2016/01/30 - 16:02 2017/02/02

Secure Connection

☒

Approve

Reject

Close

4. Click *Approve* to approve the request, or click *Reject* to reject the request.

If you approve the request, the server will start to retrieve the requested logs in the background and send them to the client. If you reject the request, the request will be canceled and the request status will be listed as *Rejected* on both the client and the server.

Fetch monitoring

The progress of an approved fetch request can be monitored on both the fetching client and the fetch server.

Go to *System Settings > Fetcher Management* and select the *Sessions* tab to monitor the fetch progress. A fetch session can be paused by clicking *Pause*, and resumed by clicking *Resume*. It can also be canceled by clicking *Cancel*.

Once the log fetching is completed, the status changes to *Done* and the request record can be deleted by clicking *Delete*. The client will start to index the logs into the database.



It can take a long time for the client to finish indexing the fetched logs and make the analyzed data available. A progress bar is shown in the GUI banner; for more information, click on it to open the *Rebuild Log Database* dialog box.

Log and report features will not be fully available until the rebuilding process is complete.

Event Log

The *Event Log* pane provides an audit log of actions made by users on FortiManager. It allows you to view log messages that are stored in memory or on the internal hard disk drive. You can use filters to search the messages and download the messages to the management computer.

See the [FortiManager Log Message Reference](#), available from the [Fortinet Document Library](#), for more information about the log messages.

Go to *System Settings > Event Log* to view the local log list.

Add Filter						
#	Date Time	Level	User	Sub Type	Description	Message
1	2018-05-29 14:20:18	notice	admin-GUI(172.18.26.1)	System manager event	CLI execution info	path=system.log-fetch.clien ^ mP34AgCu6bvsx64BD8Of /otJysxG1ckhWJSf7mPljn
2	2018-05-29 14:08:31	information	system	FortiAnalyzer system event	Configuration database object changed	[create] configuration datab
3	2018-05-29 13:36:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
4	2018-05-29 13:33:26	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
5	2018-05-29 13:33:15	information	admin	Device manager event	Device manager generic information log	Device FG-152 add succee
6	2018-05-29 13:33:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Added device FG-152 (FGV

The following options are available:

Add Filter	Filter the event log list based on the log level, user, sub type, or message. See Event log filtering on page 507 .
Download	Download the event logs in either CSV or the normal format to the management computer.
Raw Log / Formatted Log	Click on <i>Raw Log</i> to view the logs in their raw state. Click <i>Formatted Log</i> to view them in the formatted into a table.
Historical Log	Click to view the historical logs list.
Back	Click the back icon to return to the regular view from the historical view.
View	View the selected log file. This option is also available from the right-click menu, or by double-clicking on the log file. This option is only available when viewing historical event logs.
Delete	Delete the selected log file. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Clear	Clear the selected file of logs. This option is also available from the right-click menu. This option is only available when viewing historical event logs.
Type	Select the type from the dropdown list: <ul style="list-style-type: none"> <i>Event Log</i> <i>FDS Upload Log</i>: Select the device from the dropdown list. <i>FDS Download Log</i>: Select the service (<i>FDS</i>, or <i>FCT</i>) from the <i>Service</i> dropdown list, select the event type (<i>All Event</i>, <i>Push Update</i>, <i>Poll Update</i>, or <i>Manual Update</i>) from the <i>Event</i> dropdown list, and then click <i>Go</i> to browse the logs. This option is only available when viewing historical logs.
Search	Enter a search term to search the historical logs. This option is only available when viewing historical event logs.
Pagination	Browse the pages of logs and adjust the number of logs that are shown per page.

The following information is shown:

#	The log number.	
Date Time	The date and time that the log file was generated.	
Level	The log level:	
	Debug	Error
	Information	Critical
	Notification	Alert
	Warning	Emergency
User	The user that the log message relates to.	
Sub Type	The log sub-type:	
	System manager event	HA event
	FG-FM protocol event	Firmware manager event
	Device configuration event	FortiGuard service event
	Global database event	FortiClient manager event
	Script manager event	FortiMail manager event
	Web portal event	Debug I/O log event
	Firewall objects event	Configuration change event
	Policy console event	Device manager event
	VPN console event	Web service event
	Endpoint manager event	FortiAnalyzer event
	Revision history event	Log daemon event
	Deployment manager event	FIPS-CC event
	Real-time monitor event	Managed devices event
	Log and report manager event	
Description	A description of the event.	
Message	Log message details.	

Event log filtering

The event log can be filtered using the *Add Filter* box in the toolbar.

To filter FortiView summaries using the toolbar:

- Specify filters in the *Add Filter* box.
 - Regular Search: In the selected summary view, click in the *Add Filter* box, select a filter from the dropdown list, then type a value. Click NOT to negate the filter value. You can add multiple filters at a time, and connect them with an "or".
 - Advanced Search: Click the *Switch to Advanced Search* icon at the right end of the *Add Filter* box to switch to advanced search mode. In this mode, you type in the whole search criteria (log field names and values). Click the *Switch to Regular Search* icon to return to regular search.
- Click Go to apply the filter.

Task Monitor

Using the task monitor, you can view the status of the tasks you have performed.

Go to *System Settings > Task Monitor* to view the task monitor. The task list size can also be configured; see

Delete View: All						
ID	Source	Description	User	Status	Start Time	ADOM
3	Device Manager	Retrieve Device Configuration	admin		Mon Feb 6 11:52:27 2017	root
2	Install Device	Install Device	admin		Mon Feb 6 11:51:02 2017	root
< prev 1 next > (1 of 1) Total:1 Pending:0 In Progress:0 Completed (Success:1 Warning:0 Error:0) 1 ModelGate(root)[copy] (root) Copy to device done						
1	Device Manager	Add Device	admin		Mon Feb 6 11:50:51 2017	root

The following options are available:

Delete	Remove the selected task or tasks from the list. This changes to <i>Cancel Running Task(s)</i> when View is <i>Running</i> .
View	Select which tasks to view from the dropdown list, based on their status. The available options are: <i>Running</i> , <i>Pending</i> , <i>Done</i> , <i>Error</i> , <i>Cancelling</i> , <i>Cancelled</i> , <i>Aborting</i> , <i>Aborted</i> , <i>Warning</i> , and <i>All</i> .
Expand Arrow	In the <i>Source</i> column, select the expand arrow icon to display the specific actions taken under this task. To filter the specific actions taken for a task, select one of the options on top of the action list. Select the history icon to view specific information on task progress. This can be useful when troubleshooting warnings and errors.
Group Error Devices	Select <i>Group Error Devices</i> to create a group of the failed devices, allowing for re-installations to easily be done on only the failed devices.
History	Click the history icon to view task details in a new window.
Pagination	Browse the pages of tasks and adjust the number of tasks shown per page.

The following information is available:

ID	The identification number for a task.
Source	The platform from where the task is performed. Click the expand arrow to view details of the specific task and access the history button.
Description	The nature of the task. Click the arrow to display the specific actions taken under this task.
User	The user or users who performed the tasks.
Status	<p>The status of the task (hover over the icon to view the description):</p> <ul style="list-style-type: none"> • <i>Done</i>: Completed with success. • <i>Error</i>: Completed without success. • <i>Canceled</i>: User canceled the task. • <i>Canceling</i>: User is canceling the task. • <i>Aborted</i>: The FortiManager system stopped performing this task. • <i>Aborting</i>: The FortiManager system is stopping performing this task. • <i>Running</i>: Being processed. In this status, a percentage bar appears in the Status column. • <i>Pending</i> • <i>Warning</i>
Start Time	The time that the task was started.
ADOM	The ADOM associated with the task.
History	Click the history button to view task details.

SNMP

Enable the SNMP agent on the FortiManager device so it can send traps to and receive queries from the computer that is designated as its SNMP manager. This allows for monitoring the FortiManager with an SNMP manager.

SNMP has two parts - the SNMP agent that is sending traps, and the SNMP manager that monitors those traps. The SNMP communities on monitored FortiGate devices are hard coded and configured by the FortiManager system - they are not user configurable.

The FortiManager SNMP implementation is read-only — SNMP v1, v2c, and v3 compliant SNMP manager applications, such as those on your local computer, have read-only access to FortiManager system information and can receive FortiManager system traps.

SNMP agent

The SNMP agent sends SNMP traps originating on the FortiManager system to an external monitoring SNMP manager defined in a SNMP community. Typically an SNMP manager is an application on a local computer that can read the SNMP traps and generate reports or graphs from them.

The SNMP manager can monitor the FortiManager system to determine if it is operating properly, or if there are any critical events occurring. The description, location, and contact information for this FortiManager system will be part of the information an SNMP manager will have — this information is useful if the SNMP manager is monitoring many devices, and it will enable faster responses when the FortiManager system requires attention.

Go to *System Settings > Advanced > SNMP* to configure the SNMP agent.

SNMP

SNMP Agent ☒ Enable

Description

Location

Contact

SNMP v1/v2c

Community Name	Queries	Traps	Enable
Solara	✓	✓	<input checked="" type="checkbox"/>
Terminus	✓	✓	<input checked="" type="checkbox"/>
Trantor	✓	✓	<input checked="" type="checkbox"/>

SNMP v3

User Name	Security Level	Notification Hosts	Queries
Bliss	No Authentication, No Privacy		<input type="checkbox"/>
Daneel	Authentication, No Privacy		<input type="checkbox"/>
Fallom	Authentication, Privacy		<input type="checkbox"/>
Golan	No Authentication, No Privacy		<input type="checkbox"/>

The following information and options are available:

SNMP Agent	Select to enable the SNMP agent. When this is enabled, it sends FortiManager SNMP traps.
Description	Optionally, type a description of this FortiManager system to help uniquely identify this unit.
Location	Optionally, type the location of this FortiManager system to help find it in the event it requires attention.
Contact	Optionally, type the contact information for the person in charge of this FortiManager system.
SNMP v1/v2c	The list of SNMP v1/v2c communities added to the FortiManager configuration.
Create New	Select <i>Create New</i> to add a new SNMP community. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v1/v2c communities on page 511 .
Edit	Edit the selected SNMP community.
Delete	Delete the selected SNMP community or communities.
Community Name	The name of the SNMP community.

Queries	The status of SNMP queries for each SNMP community. The enabled icon indicates that at least one query is enabled. The disabled icon indicates that all queries are disabled.
Traps	The status of SNMP traps for each SNMP community. The enabled icon indicates that at least one trap is enabled. The disabled icon indicates that all traps are disabled.
Enable	Enable or disable the SNMP community.
SNMP v3	The list of SNMPv3 users added to the configuration.
Create New	Select <i>Create New</i> to add a new SNMP user. If SNMP agent is not selected, this control will not be visible. For more information, see SNMP v3 users on page 514 .
Edit	Edit the selected SNMP user.
Delete	Delete the selected SNMP user or users.
User Name	The user name for the SNMPv3 user.
Security Level	The security level assigned to the SNMPv3 user.
Notification Hosts	The notification host or hosts assigned to the SNMPv3 user.
Queries	The status of SNMP queries for each SNMP user. The enabled icon indicates queries are enabled. The disabled icon indicates they are disabled.

SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. You must configure your FortiManager to belong to at least one SNMP community so that community's SNMP managers can query the FortiManager system information and receive SNMP traps from it.



These SNMP communities do not refer to the FortiGate devices the FortiManager system is managing.

Each community can have a different configuration for SNMP traps and can be configured to monitor different events. You can add the IP addresses of up to eight hosts to each community. Hosts can receive SNMP device traps and information.

To create a new SNMP community:

1. Go to *System Settings > Advanced > SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v1/v2c* section, click *Create New* in the toolbar. The *New SNMP Community* pane opens.

New SNMP Community

Name:

Hosts:

IP Address/Netmask	Interface	Delete
<input type="button" value="Add"/>		

Queries:

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Port	Enable
v1	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
High licensed device quota	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

3. Configure the following options, then click *OK* to create the community.

Name	Enter a name to identify the SNMP community. This name cannot be edited later.
Hosts	<p>The list of hosts that can use the settings in this SNMP community to monitor the FortiManager system.</p> <p>When you create a new SNMP community, there are no host entries. Select <i>Add</i> to create a new entry that broadcasts the SNMP traps and information to the network connected to the specified interface.</p>
IP Address/Netmask	<p>Enter the IP address and netmask of an SNMP manager.</p> <p>By default, the IP address is 0.0.0.0 so that any SNMP manager can use this SNMP community.</p>
Interface	Select the interface that connects to the network where this SNMP manager is located from the dropdown list. This must be done if the SNMP manager is on the Internet or behind a router.
Delete	Click the delete icon to remove this SNMP manager entry.
Add	Select to add another entry to the Hosts list. Up to eight SNMP manager entries can be added for a single community.

Queries	Enter the port number (161 by default) the FortiManager system uses to send v1 and v2c queries to the FortiManager in this community. Enable queries for each SNMP version that the FortiManager system uses.
Traps	Enter the Remote port number (162 by default) the FortiManager system uses to send v1 and v2c traps to the FortiManager in this community. Enable traps for each SNMP version that the FortiManager system uses.
SNMP Event	<p>Enable the events that will cause SNMP traps to be sent to the community.</p> <ul style="list-style-type: none"> • <i>Interface IP changed</i> • <i>Log disk space low</i> • <i>CPU Overuse</i> • <i>Memory Low</i> • <i>System Restart</i> • <i>CPU usage exclude NICE threshold</i> • <i>HA Failover</i> • <i>RAID Event</i> (only available for devices that support RAID) • <i>Power Supply Failed</i> (only available on supported hardware devices) <p>FortiAnalyzer feature set SNMP events:</p> <ul style="list-style-type: none"> • <i>High licensed device quota</i> • <i>High licensed log GB/day</i> • <i>Log Alert</i> • <i>Log Rate</i> • <i>Data Rate</i>

To edit an SNMP community:

1. Go to *System Settings > Advanced > SNMP*.
2. In the *SNMP v1/v2c* section, double-click on a community, right-click on a community then select *Edit*, or select a community then click *Edit* in the toolbar. The *Edit SNMP Community* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP community or communities:

1. Go to *System Settings > Advanced > SNMP*.
2. In the *SNMP v1/v2c* section, select the community or communities you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected community or communities.

SNMP v3 users

The FortiManager SNMP v3 implementation includes support for queries, traps, authentication, and privacy. SNMP v3 users can be created, edited, and deleted as required.

To create a new SNMP user:

1. Go to *System Settings > Advanced > SNMP* and ensure the SNMP agent is enabled.
2. In the *SNMP v3* section, click *Create New* in the toolbar. The *New SNMP User* pane opens.

New SNMP User

User Name:

Security Level: No Authentication, No Privacy

Queries: ☐ Enable Port: 161

Notification Hosts: 0.0.0.0 +

SNMP Event	Enable
Interface IP changed	<input checked="" type="checkbox"/>
Log Disk Space Low	<input checked="" type="checkbox"/>
CPU Overuse	<input checked="" type="checkbox"/>
Memory Low	<input checked="" type="checkbox"/>
System Restart	<input checked="" type="checkbox"/>
CPU usage exclude NICE threshold	<input checked="" type="checkbox"/>
HA Failover	<input checked="" type="checkbox"/>
High licensed device quota	<input checked="" type="checkbox"/>
High licensed log GB/day	<input checked="" type="checkbox"/>
Log Alert	<input checked="" type="checkbox"/>
Log Rate	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="checkbox"/>

OK Cancel

3. Configure the following options, then click *OK* to create the community.

User Name	The name of the SNMP v3 user.
Security Level	<p>The security level of the user. Select one of the following:</p> <ul style="list-style-type: none"> • <i>No Authentication, No Privacy</i> • <i>Authentication, No Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5) and enter the password. • <i>Authentication, Privacy</i>: Select the <i>Authentication Algorithm</i> (SHA1, MD5), the <i>Private Algorithm</i> (AES, DES), and enter the passwords.
Queries	Select to enable queries then enter the port number. The default port is 161.
Notification Hosts	The IP address or addresses of the host. Click the add icon to add multiple IP addresses.

SNMP Event

Enable the events that will cause SNMP traps to be sent to the SNMP manager.

- *Interface IP changed*
- *Log disk space low*
- *CPU Overuse*
- *Memory Low*
- *System Restart*
- *CPU usage exclude NICE threshold*
- *HA Failover*
- *RAID Event* (only available for devices that support RAID)
- *Power Supply Failed* (only available on supported hardware devices)

FortiAnalyzer feature set SNMP events:

- *High licensed device quota*
- *High licensed log GB/day*
- *Log Alert*
- *Log Rate*
- *Data Rate*

To edit an SNMP user:

1. Go to *System Settings > Advanced > SNMP*.
2. In the *SNMP v3* section, double-click on a user, right-click on a user then select *Edit*, or select a user then click *Edit* in the toolbar. The *Edit SNMP User* pane opens.
3. Edit the settings as required, then click *OK* to apply your changes.

To delete an SNMP user or users:

1. Go to *System Settings > Advanced > SNMP*.
2. In the *SNMP v3* section, select the user or users you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation dialog box to delete the selected user or users.

SNMP MIBs

The Fortinet and FortiManager MIBs, along with the two RFC MIBs, can be obtained from Customer Service & Support (<https://support.fortinet.com>). You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER-MIB.mib* MIB file in the firmware image file folder. The *FORTINET-CORE-MIB.mib* file is located in the main FortiManager 5.00 file folder.

RFC support for SNMP v3 includes Architecture for SNMP Frameworks (RFC 3411), and partial support of User-based Security Model (RFC 3414).

To be able to communicate with the SNMP agent, you must include all of these MIBs into your SNMP manager. Generally your SNMP manager will be an application on your local computer. Your SNMP manager might already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet and FortiManager proprietary MIBs to this database.

MIB file name or RFC	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor Fortinet unit configuration settings and receive traps from the Fortinet SNMP agent.
FORTINET-FORTIMANAGER-MIB.mib	The proprietary FortiManager MIB includes system information and trap information for FortiManager units.
RFC-1213 (MIB II)	The Fortinet SNMP agent supports MIB II groups with the following exceptions. <ul style="list-style-type: none"> No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10). Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.
RFC-2665 (Ethernet-like MIB)	The Fortinet SNMP agent supports Ethernet-like MIB information with the following exception. No support for the dot3Tests and dot3Errors groups.

SNMP traps

Fortinet devices share SNMP traps, but each type of device also has traps specific to that device type. For example FortiManager units have FortiManager specific SNMP traps. To receive Fortinet device SNMP traps, you must load and compile the FORTINET-CORE-MIB into your SNMP manager.

Traps sent include the trap message as well as the unit serial number (fnSysSerial) and host name (sysName). The Trap Message column includes the message that is included with the trap, as well as the SNMP MIB field name to help locate the information about the trap.

Trap message	Description
ColdStart, WarmStart, LinkUp, LinkDown	Standard traps as described in RFC 1215.
CPU usage high (fnTrapCpuThreshold)	CPU usage exceeds the set percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-high-cpu-threshold <percentage value> end</pre>

Trap message	Description
CPU usage excluding NICE processes (fnSysCpuUsageExcludedNice)	CPU usage excluding NICE processes exceeds the set percentage. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-cpu-high-exclude-nice-threshold <percentage value> end</pre>
Memory low (fnTrapMemThreshold)	Memory usage exceeds 90 percent. This threshold can be set in the CLI using the following commands: <pre>config system snmp sysinfo set trap-low-memory-threshold <percentage value> end</pre>
Log disk too full (fnTrapLogDiskThreshold)	Log disk usage has exceeded the configured threshold. Only available on devices with log disks.
Temperature too high (fnTrapTempHigh)	A temperature sensor on the device has exceeded its threshold. Not all devices have thermal sensors. See manual for specifications.
Voltage outside acceptable range (fnTrapVoltageOutOfRange)	Power levels have fluctuated outside of normal levels. Not all devices have voltage monitoring instrumentation.
Power supply failure (fnTrapPowerSupplyFailure)	Power supply failure detected. Available on some devices that support redundant power supplies.
Interface IP change (fnTrapIpChange)	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the Fortinet unit. You can use this trap to track interface IP address changes for interfaces with dynamic IP addresses set using DHCP or PPPoE.
HA switch (fnTrapHASwitch)	FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Fortinet & FortiManager MIB fields

The Fortinet MIB contains fields reporting current Fortinet unit status information. The below tables list the names of the MIB fields and describe the status information available for each one. You can view more details about the information available from all Fortinet MIB fields by compiling the `fortinet.3.00.mib` file into your SNMP manager and browsing the Fortinet MIB fields.

System MIB fields:

MIB field	Description
fnSysSerial	Fortinet unit serial number.

Administrator accounts:

MIB field	Description
fnAdminNumber	The number of administrators on the Fortinet unit.
fnAdminTable	Table of administrators.
fnAdminIndex	Administrator account index number.
fnAdminName	The user name of the administrator account.
fnAdminAddr	An address of a trusted host or subnet from which this administrator account can be used.
fnAdminMask	The netmask for fnAdminAddr.

Custom messages:

MIB field	Description
fnMessages	The number of custom messages on the Fortinet unit.

MIB fields and traps

MIB field	Description
fmModel	A table of all FortiManager models.
fmTrapHASwitch	The FortiManager HA cluster has been re-arranged. A new master has been selected and asserted.

Mail Server

A mail server allows the FortiManager to send email messages, such as notifications when reports are run or specific events occur. Mail servers can be added, edited, deleted, and tested.

Go to *System Settings > Advanced > Mail Server* to configure SMTP mail server settings.



If an existing mail server is in use, the delete icon is removed and the mail server entry cannot be deleted.

To add a mail server:

1. Go to *System Settings > Advanced > Mail Server*.
2. Click *Create New* in the toolbar. The *Create New Mail Server Settings* pane opens.

Create New Mail Server Settings

SMTP Server Name

Mail Server

SMTP Server Port

Enable Authentication ☐

E-Mail Account

Password

3. Configure the following settings and then select *OK* to create the mail server.

SMTP Server Name	Enter a name for the SMTP server.
Mail Server	Enter the mail server information.
SMTP Server Port	Enter the SMTP server port number. The default port is 25.
Enable Authentication	Select to enable authentication.
Email Account	Enter an email account. This option is only accessible when authentication is enabled.
Password	Enter the email account password. This option is only accessible when authentication is enabled.

To edit a mail server:

1. Go to *System Settings > Advanced > Mail Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Mail Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the mail server:

1. Go to *System Settings > Advanced > Mail Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
4. Type the email address you would like to send a test email to and click *OK*. A confirmation or failure message will be displayed.
5. Click *OK* to close the confirmation dialog box.

To delete a mail server or servers:

1. Go to *System Settings > Advanced > Mail Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server.

Syslog Server

Go to *System Settings > Advanced > Syslog Server* to configure syslog server settings. Syslog servers can be added, edited, deleted, and tested.



If an existing syslog server is in use, the delete icon is removed and the server entry cannot be deleted.

To add a syslog server:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Click *Create New* in the toolbar. The *Create New Syslog Server Settings* pane opens.

Create New Syslog Server Settings

Name

IP address (or FQDN)

Syslog Server Port

3. Configure the following settings and then select *OK* to create the mail server.

Name	Enter a name for the syslog server.
IP address (or FQDN)	Enter the IP address or FQDN of the syslog server.
Syslog Server Port	Enter the syslog server port number. The default port is 514.

To edit a syslog server:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Double-click on a server, right-click on a server and then select *Edit* from the menu, or select a server then click *Edit* in the toolbar. The *Edit Syslog Server Settings* pane opens.
3. Edit the settings as required, and then click *OK* to apply the changes.

To test the syslog server:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Select the server you need to test.
3. Click *Test* from the toolbar, or right-click and select *Test*.
A confirmation or failure message will be displayed.

To delete a syslog server or servers:

1. Go to *System Settings > Advanced > Syslog Server*.
2. Select the server or servers you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click *OK* in the confirmation box to delete the server or servers.

Meta Fields

Meta fields allow administrators to add extra information when configuring, adding, or maintaining FortiGate units or adding new administrators. You can make the fields mandatory or optional, and set the length of the field.

With the fields set as mandatory, administrators must supply additional information when they create a new FortiGate object, such as an administrator account or firewall policy. Fields for this new information are added to the FortiGate unit dialog boxes in the locations where you create these objects. You can also provide fields for optional additional information.

The one exception to this is the *System Administrators* object. This object applies only to administrators on the FortiManager unit. All other objects are related to FortiGate units.

Go to *System Settings > Advanced > Meta Fields* to configure meta fields. Meta fields can be added, edited, and deleted.

+ Create New Edit Delete Expand All Collapse All			
<input type="checkbox"/> ▲ Meta Fields	Length	Importance	Status
▼ System Administrator (2)			
<input type="checkbox"/> Contact Email	50	Optional	Enabled
<input type="checkbox"/> Contact Phone	50	Optional	Enabled
▼ Device (5)			
<input type="checkbox"/> City	50	Optional	Enabled
<input type="checkbox"/> Company/Organization	50	Optional	Enabled
<input type="checkbox"/> Contact	50	Optional	Enabled
<input type="checkbox"/> Country	50	Optional	Enabled
<input type="checkbox"/> Province/State	50	Optional	Enabled
▼ Device Group			
▼ Administrative Domain			
▼ Firewall Address			
▼ Firewall Address Group			
▼ Firewall Service			
▼ Firewall Service Group			
▼ Firewall Policy			



Select *Expand All* or *Contract All* from the toolbar or right-click menu to view all of or none of the meta fields under each object.

To create a new meta field:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Click *Create New* in the toolbar. The *Create New Meta Field* pane opens.

Create New Meta Fields

Object

Devices

Name

Length

20

Importance

☐ Optional
 ☒ Required

Status

☐ Disabled
 ☒ Enabled

OK

Cancel

3. Configure the following settings and then select **OK** to create the meta field.

Object	The object this metadata field applies to: <i>System Administrators, Devices, Device Groups, Chassis, Administrative Domain, Firewall Addresses, Firewall Address Groups, Firewall Services, Firewall Service Groups, or Firewall Policy.</i>
Name	Enter the label to use for the field.
Length	Select the maximum number of characters allowed for the field from the dropdown list: <i>20, 50, or 255.</i>
Importance	Select <i>Required</i> to make the field compulsory, otherwise select <i>Optional</i> .
Status	Select <i>Disabled</i> to disable this field. The default selection is <i>Enabled</i> . This field is only available for non-firewall objects.

To edit a meta field:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Double-click on a field, right-click on a field and then select *Edit* from the menu, or select a field then click *Edit* in the toolbar. The *Edit Meta Fields* pane opens.
3. Edit the settings as required, and then click **OK** to apply the changes.



The *Object* and *Name* fields cannot be edited.

To delete a meta field or fields:

1. Go to *System Settings > Advanced > Meta Fields*.
2. Select the field or fields you need to delete.
3. Click *Delete* in the toolbar, or right-click and select *Delete*.
4. Click **OK** in the confirmation box to delete the field or fields.



The default meta fields cannot be deleted.

Device logs

The FortiManager allows you to log system events to disk. You can control device log file size and the use of the FortiManager unit's disk space by configuring log rolling and scheduled uploads to a server.

As the FortiManager unit receives new log items, it performs the following tasks:

- Verifies whether the log file has exceeded its file size limit.
- Checks to see if it is time to roll the log file if the file size is not exceeded.

When a current log file (`tlog.log`) reaches its maximum size, or reaches the scheduled time, the FortiManager unit rolls the active log file by renaming the file. The file name will be in the form of `xlog.N.log` (for example, `tlog.1252929496.log`), where `x` is a letter indicating the log type and `N` is a unique number corresponding to the time the first log entry was received. The file modification time will match the time when the last log was received in the log file.

Once the current log file is rolled into a numbered log file, it will not be changed. New logs will be stored in the new current log called `tlog.log`. If log uploading is enabled, once logs are uploaded to the remote server or downloaded via the GUI, they are in the following format:

```
FG3K6A3406600001-tlog.1252929496.log-2017-09-29-08-03-54.gz
```

If you have enabled log uploading, you can choose to automatically delete the rolled log file after uploading, thereby freeing the amount of disk space used by rolled log files. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Log rolling and uploading can be enabled and configured using the GUI or CLI.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features](#) on page 390.

Configuring rolling and uploading of logs using the GUI

Go to *System Settings > Advanced > Device Log Setting* to configure device log settings.

Device Log Settings

Registered Device Logs

Roll log file when size exceeds (10-500)MB
☒ Roll log files at scheduled time
 Hour Minute
☒ Upload logs using a standard file transfer protocol
Upload Server Type
Upload Server IP
User Name
Password
Remote Directory
Upload Log Files ☒ When rolled ☐ Daily at Hour
☐ Upload log files in gzip file format
☐ Delete log files after uploading

Local Device Log

☒ Send the local event logs to FortiAnalyzer/FortiManager
IP Address
Upload Option ☒ Real-time ☐ Schedule Time
Severity Level
☐ Secure connection for log transmission

Apply

Configure the following settings, and then select *Apply*:

Registered Device Logs	
Roll log file when size exceeds	Enter the log file size, from 10 to 500MB. Default: 200MB.
Roll log files at scheduled time	Select to roll logs daily or weekly. <ul style="list-style-type: none"> • <i>Daily</i>: select the hour and minute value in the dropdown lists. • <i>Weekly</i>: select the day, hour, and minute value in the dropdown lists.
Upload logs using a standard file transfer protocol	Select to upload logs and configure the following settings.
Upload Server Type	Select one of <i>FTP</i> , <i>SFTP</i> , or <i>SCP</i> .
Upload Server IP	Enter the IP address of the upload server.
User Name	Enter the username used to connect to the upload server.
Password	Enter the password used to connect to the upload server.
Remote Directory	Enter the remote directory on the upload server where the log will be uploaded.
Upload Log Files	Select to upload log files when they are rolled according to settings selected under <i>Roll Logs</i> , or daily at a specific hour.
Upload rolled files in gzip file format	Select to gzip the logs before uploading. This will result in smaller logs and faster upload times.
Delete files after uploading	Select to remove device log files from the FortiManager system after they have been uploaded to the Upload Server.
Local Device Log	
Send the local event logs to FortiAnalyzer / FortiManager	Select to send local event logs to another FortiAnalyzer or FortiManager device.
IP Address	Enter the IP address of the FortiAnalyzer or FortiManager.
Upload Option	Select to upload logs in real time or at a scheduled time. When selecting a scheduled time, you can specify the hour and minute to upload logs each day.
Severity Level	Select the minimum log severity level from the dropdown list. This option is only available when <i>Upload Option</i> is <i>Realtime</i> .
Secure connection for log transmission	Select to use a secure connection for log transmission.

Configuring rolling and uploading of logs using the CLI

Log rolling and uploading can be enabled and configured using the CLI. For more information, see the [FortiManager CLI Reference](#).

Enable or disable log file uploads

Use the following CLI commands to enable or disable log file uploads.

To enable log uploads:

```
config system log settings
  config rolling-regular
    set upload enable
  end
```

To disable log uploads:

```
config system log settings
  config rolling-regular
    set upload disable
  end
```

Roll logs when they reach a specific size

Use the following CLI commands to specify the size, in MB, at which a log file is rolled.

To roll logs when they reach a specific size:

```
config system log settings
  config rolling-regular
    set file-size <integer>
  end
```

Roll logs on a schedule

Use the following CLI commands to configure rolling logs on a set schedule, or never.

To disable log rolling:

```
config system log settings
  config rolling-regular
    set when none
  end
```

To enable daily log rolling:

```
config system log settings
  config rolling-regular
    set upload enable
    set when daily
```

```

    set hour <integer>
    set min <integer>
end

```

To enable weekly log rolling:

```

config system log settings
config rolling-regular
    set when weekly
    set days {mon | tue | wed | thu | fri | sat | sun}
    set hour <integer>
    set min <integer>
end

```

File Management

FortiManager allows you to configure automatic deletion of device log files, quarantined files, reports, and content archive files after a set period of time.

Go to *System Settings > Advanced > File Management* to configure file management settings.

File Management

Automatically Delete

<input type="checkbox"/> Device log files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Reports older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Content archive files older than	365	Days	Scheduled daily at time	00:00
<input type="checkbox"/> Quarantined files older than	365	Days	Scheduled daily at time	00:00

Apply

Configure the following settings, and then select *Apply*:

Device log files older than	Select to enable automatic deletion of compressed log files. Enter a value in the text field, select the time period (<i>Days</i> , <i>Weeks</i> , or <i>Months</i>), and choose a time of day.
Reports older than	Select to enable automatic deletion of reports of data from compressed log files. Enter a value in the text field, select the time period, and choose a time of day.
Content archive files older than	Select to enable automatic deletion of IPS and DP archives from Archive logs. Enter a value in the text field, select the time period, and choose a time of day.
Quarantined files older than	Select to enable automatic deletion of compressed log files of quarantined files. Enter a value in the text field, select the time period, and choose a time of day.

The time period you select determines how often the item is checked. If you select *Months*, then the item is checked once per month. If you select *Weeks*, then the item is checked once per week, and so on. For example, if you specify *Device log files older than 3 Months*, then on July 1, the logs for April, May, and June are kept and the logs for March and older are deleted.



This pane is only available when the FortiAnalyzer features are manually enabled. For more information, see [FortiAnalyzer Features on page 390](#).

Advanced Settings

Go to *System Settings > Advanced > Advanced Settings* to view and configure advanced settings and download WSDL files.

Configure the following settings and then select *Apply*:

Offline Mode	Enabling <i>Offline Mode</i> shuts down the protocol used to communicate with managed devices. This allows you to configure, or troubleshoot, the FortiManager without affecting managed devices. The FortiManager cannot automatically connect to a FortiGate if offline mode is enabled.
ADOM Mode	Select the ADOM mode, either <i>Normal</i> or <i>Advanced</i> . Advanced mode will allow you to assign a VDOM from a single device to a different ADOM, but will result in more complicated management scenarios. It is recommended only for advanced users.
Download WSDL file	Select the required WSDL functions then click the <i>Download</i> button to download the WSDL file to your management computer. When selecting <i>Legacy Operations</i> , no other options can be selected. Web services is a standards-based, platform independent, access method for other hardware and software APIs. The file itself defines the format of commands the FortiManager will accept as well as the responses to expect. Using the WSDL file, third-party or custom applications can communicate with the FortiManager unit and operate it or retrieve information, just as an administrator can from the GUI or CLI.
Chassis Management	Enable chassis management, then enter the chassis update interval, from 4 to 1440 minutes. Default: 15 minutes.
Configuration Changes Received from FortiGate	Select to either automatically accept changes (default) or to prompt the administrator to accept the changes.
Task List Size	Set a limit on the size of the task list. Default: 2000.
Verify Installation	Select to preview the installation before proceeding.
Allow Install Interface Policy Only	Select to manage and install only interface based policies, instead of all device and policy configuration.
Policy Hit Count	Enable or disable policy hit counting.
Display Policy & Objects in Dual Pane	Enable to display both the <i>Policy Packages</i> and <i>Object Configurations</i> tabs on a single pane in the <i>Policy & Objects</i> module. See Display options on page 216 .

Display Device/Group tree view in Device Manager

Enable to display devices and groups within a single tree menu and include *Add Device* and *Install Wizard* commands in the right click menu.



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.